

PCI Scan Vulnerability Report

PCI Status

The following table highlights the overall compliance status and each individual system's compliance status. Following the table is a detailed report specifying each system and its specific vulnerabilities.

Overall PCI Status		FAIL
Live IP Address Scanned	Security Risk Rating	PCI Status
185.132.38.51	<div><div></div><div></div><div></div><div></div><div></div></div>	FAIL

Report Summary	
Company:	WWW.WINGPATH.CO.UK
Hosts in account	1
Hosts scanned	1
Hosts active	1
Scan date	May 16, 2024
Report date	May 16, 2024

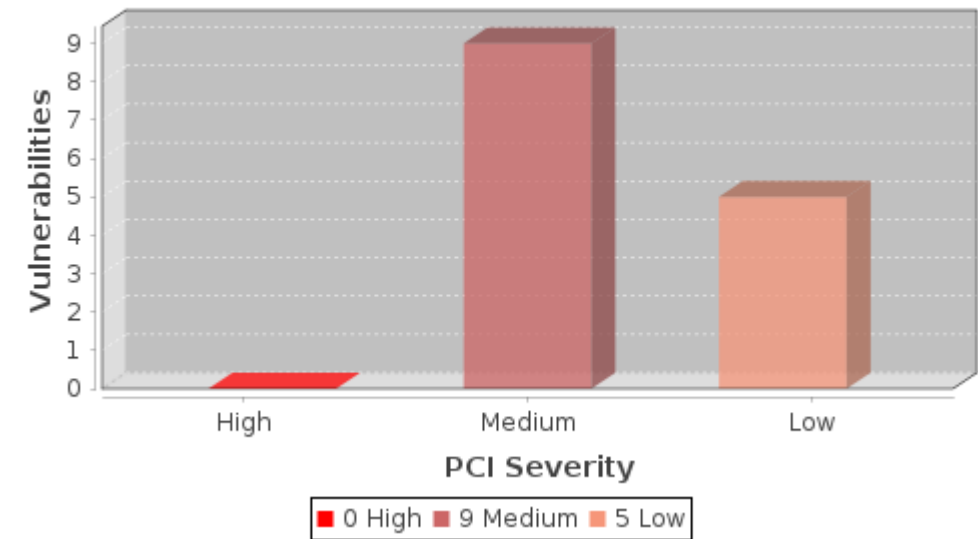
Summary of Vulnerabilities

Vulnerabilities total:	165	Security risk:	<div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div><div></div></div>	5
------------------------	-----	----------------	---	---

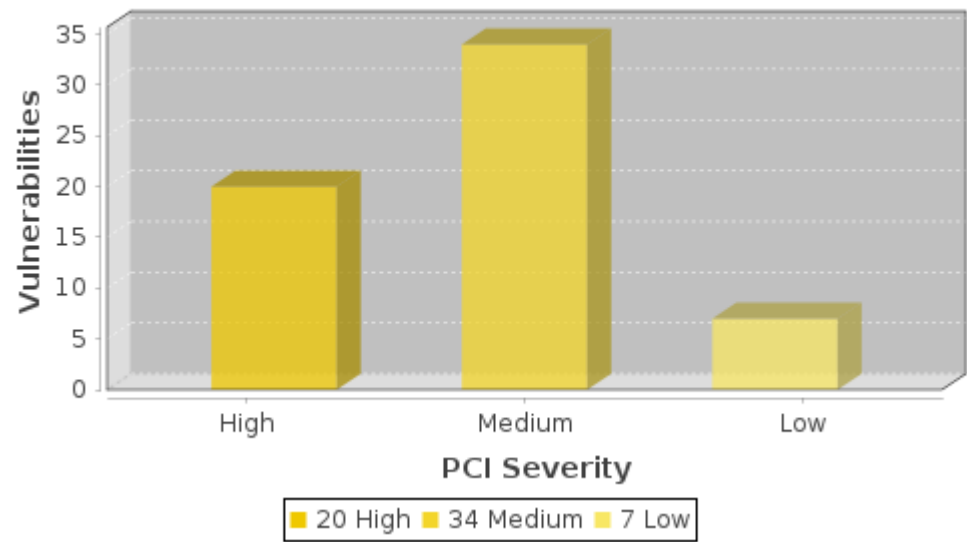
by Severity				
Severity	Confirmed	Potential	Information gathered	Total
5	2	5	0	7
4	2	28	0	30
3	2	16	5	23
2	7	12	8	27
1	1	0	77	78
Total	14	61	90	165

by PCI Severity			
PCI Severity	Confirmed	Potential	Total
High	0	20	20
Medium	9	34	43
Low	5	7	12
Total	14	61	75

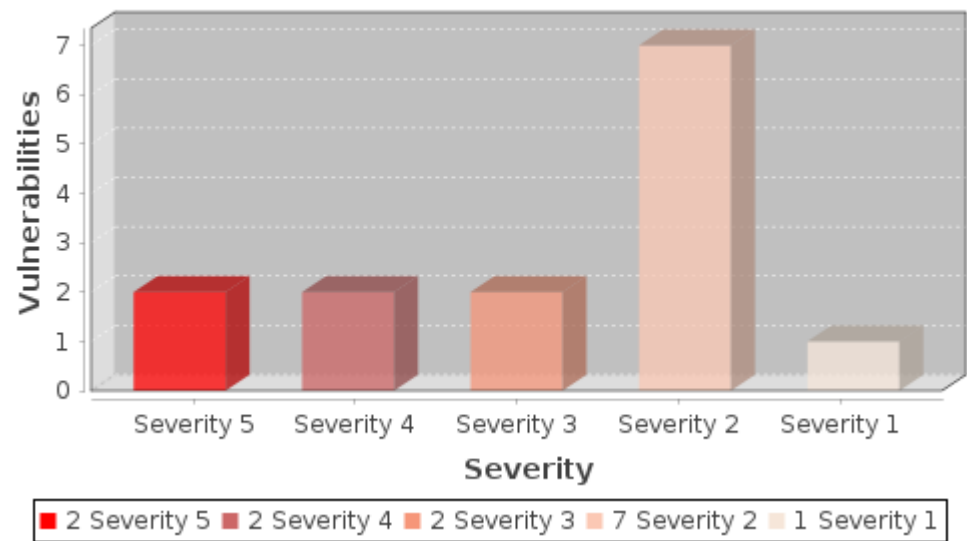
Vulnerabilities by PCI Severity

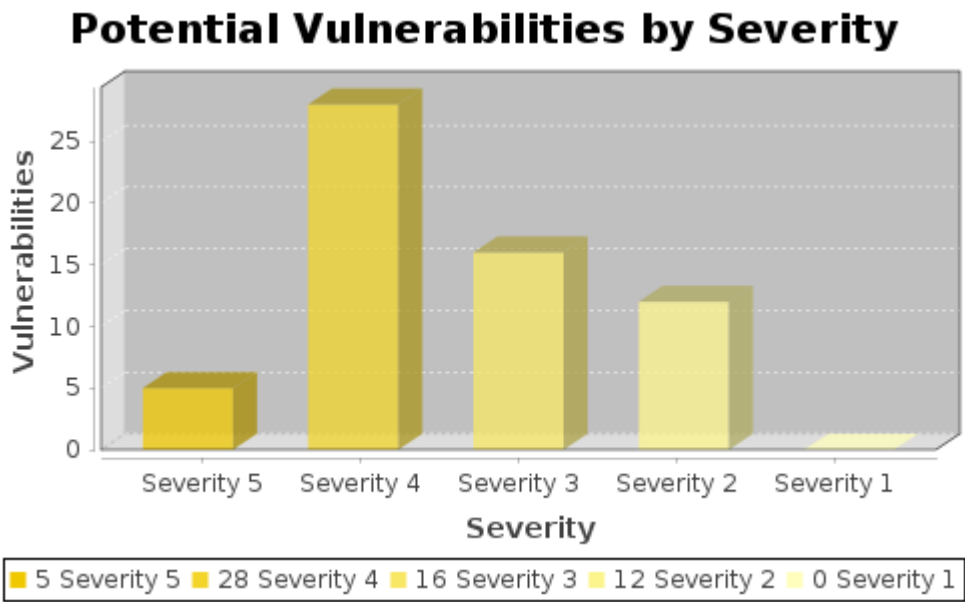


Potential Vulnerabilities by PCI Severity



Vulnerabilities by Severity





Detailed Results

185.132.38.51 (basil.wingpath.co.uk,)

Ubuntu/Linux

Vulnerabilities total:	165	Security risk:	<div><div></div><div></div><div></div><div></div><div></div></div>	5
------------------------	-----	----------------	--	---

Vulnerabilities (14)

Reflected Cross-Site Scripting (XSS) Vulnerabilities

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

Automatic Failure: Cross-site Scripting (XSS) vulnerability
The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score: 3.9 E:H/RL:U/RC:UC
Severity: 5
QID: 150001
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2022-03-09 13:28:17.0

THREAT:

XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

IMPACT:

XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used as a part of a compromise.

SOLUTION:

Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

RESULT:

url: https://wingpath.co.uk/upgrade.php?product=modsnmp%22%3E%3CDIV%20STYLE%3D%22width%3Aexpression(qssmWB2pAX5%3D7)%22%3E

Tested parameter: product

Payload: product=modsnmp%22%3E%3CDIV%20STYLE%3D%22width%3Aexpression(qssmWB2pAX5%3D7)%22%3E

variants: 35

comment:

Response content-type: text/html

```
matched: incolumnl"><div id="maincontent">
<h2>Upgrade a product</h2>

<p>If you want to upgrade to a later version of a product (e.g. from
Modsak 2 to
Modsak 3),
you should use the
<a class="link" href="upgradev.php?product=modsnmp"><DIV STYLE="width:expression(qssmWB2pAX5=7)">">version upgrade form</a>.
</p>

<p>If you want to upgrade to a less restrictive licence for the same version
of a product (e.g. from
ModSnmp-300 to
ModSnmp-600),
you should use the
<a class="link" href="upgradel.php?product=
```

Reflected Cross-Site Scripting (XSS) Vulnerabilities

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

Automatic Failure: Cross-site Scripting (XSS) vulnerability
The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	3.9 E:H/RL:U/RC:UC
Severity:	5 <div></div>
QID:	150001
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-03-09 13:28:17.0

THREAT:

XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

IMPACT:

XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used to as a part of a compromise.

SOLUTION:

Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

RESULT:

url: https://wingpath.co.uk/upgrade.php?product=modsnmp%22%3E%3CDIV%20STYLE%3D%22width%3Aexpression(qss31vrW4I7%3D7)%22%3E

Tested parameter: product

Payload: product=modsnmp%22%3E%3CDIV%20STYLE%3D%22width%3Aexpression(qss31vrW4I7%3D7)%22%3E

variants: 35

comment:

Response content-type: text/html

matched: incolumnl"><div id="maincontent">

<h2>Upgrade a product</h2>

<p>If you want to upgrade to a later version of a product (e.g. from

Modsak 2 to

Modsak 3),

you should use the

<DIV STYLE="width:expression(qss31vrW4I7=7)">">version upgrade form.

</p>

<p>If you want to upgrade to a less restrictive licence for the same version

of a product (e.g. from

ModSnmp-300 to

ModSnmp-600),

you should use the

<a class="link" href="upgradel.php?product=

SSH Prefix Truncation Vulnerability (Terrapin)

port 22 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score: 6.4 AV:N/AC:L/Au:N/C:P/I:P/A:N

CVSS Temporal Score: 5.0 E:POC/RL:OF/RC:C

Severity: 4

QID: 38913

Category: General remote services

CVE ID: CVE-2023-48795

Vendor Reference: OpenSSH Advisory

Bugtraq ID: -

Last Update: 2024-04-20 00:00:01.0

THREAT:
The Terrapin attack exploits weaknesses in the SSH transport layer protocol in combination with newer cryptographic algorithms and encryption modes introduced by OpenSSH over 10 years ago. Since then, these have been adopted by a wide range of SSH implementations, therefore affecting a majority of current implementations.

QID Detection Logic (Unauthenticated):
This detection attempts to start the SSH key exchange process and examines whether either of the vulnerable ChaCha20-Poly1305 Algorithm or CBC-EtM Algorithm is active. It subsequently verifies whether Strict Key Exchange is enabled. If a target is identified as vulnerable, it indicates that the target supports either of the vulnerable algorithms and lacks support for Strict Key Exchange.

IMPACT:
Successful exploitation of the vulnerability may allow an attacker to downgrade the security of an SSH connection when using SSH extension negotiation. The impact in practice heavily depends on the supported extensions. Most commonly, this will impact the security of client authentication when using an RSA public key.

SOLUTION:
Customers are advised to refer to the individual vendor advisory for their operating system and install the patch released by the vendor. For more information regarding the vulnerability, please refer to [Terrapin Vulnerability](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[OpenWall Security Advisory](#)

RESULT:
SSH Prefix Truncation Vulnerability (Terrapin) detected on port: 22
ChaCha20-Poly1305 Algorithm Support: True
CBC-EtM Algorithm Support: False
Strict Key Exchange algorithm enabled: False

SSL Server Allows Anonymous Authentication Vulnerability

port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	5.1 AV:N/AC:H/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	4.1 E:U/RL:W/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38142
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-25 17:36:07.0

THREAT:
The Secure Socket Layer (SSL) protocol allows for secure communication between a client and a server. The client usually authenticates the server using an algorithm like RSA or DSS. Some SSL ciphers allow SSL communication without authentication. Most common Web browsers like Microsoft Internet Explorer, Netscape and Mozilla do not use anonymous authentication ciphers by default.

A vulnerability exists in SSL communications when clients are allowed to connect using no authentication algorithm. SSL client-server communication may use several different types of authentication: RSA, Diffie-Hellman, DSS or none. When 'none' is used, the communications are vulnerable to a man-in-the-middle attack."

IMPACT:

An attacker can exploit this vulnerability to impersonate your server to clients.

SOLUTION:

Disable support for anonymous authentication to mitigate this vulnerability.

RESULT:

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH)

GRADE

TLSv1 SUPPORTS CIPHERS WITH NO AUTHENTICATION
ADH-AES128-SHA DH None SHA1 AES(128) MEDIUM
ADH-AES256-SHA DH None SHA1 AES(256) HIGH
ADH-CAMELLIA128-SHA DH None SHA1 Camellia(128) MEDIUM
ADH-CAMELLIA256-SHA DH None SHA1 Camellia(256) HIGH
ADH-SEED-SHA DH None SHA1 SEED(128) MEDIUM
AECDH-AES128-SHA ECDH None SHA1 AES(128) MEDIUM
AECDH-AES256-SHA ECDH None SHA1 AES(256) HIGH
TLSv1.1 SUPPORTS CIPHERS WITH NO AUTHENTICATION
ADH-AES128-SHA DH None SHA1 AES(128) MEDIUM
ADH-AES256-SHA DH None SHA1 AES(256) HIGH
ADH-CAMELLIA128-SHA DH None SHA1 Camellia(128) MEDIUM
ADH-CAMELLIA256-SHA DH None SHA1 Camellia(256) HIGH
ADH-SEED-SHA DH None SHA1 SEED(128) MEDIUM
AECDH-AES128-SHA ECDH None SHA1 AES(128) MEDIUM
AECDH-AES256-SHA ECDH None SHA1 AES(256) HIGH
TLSv1.2 SUPPORTS CIPHERS WITH NO AUTHENTICATION
ADH-AES128-SHA DH None SHA1 AES(128) MEDIUM
ADH-AES256-SHA DH None SHA1 AES(256) HIGH
ADH-CAMELLIA128-SHA DH None SHA1 Camellia(128) MEDIUM
ADH-AES128-SHA256 DH None SHA256 AES(128) MEDIUM
ADH-AES256-SHA256 DH None SHA256 AES(256) HIGH
ADH-CAMELLIA256-SHA DH None SHA1 Camellia(256) HIGH
ADH-SEED-SHA DH None SHA1 SEED(128) MEDIUM
ADH-AES128-GCM-SHA256 DH None AEAD AESGCM(128) MEDIUM
ADH-AES256-GCM-SHA384 DH None AEAD AESGCM(256) HIGH
ADH-CAMELLIA128-SHA256 DH None SHA256 Camellia(128) MEDIUM
ADH-CAMELLIA256-SHA256 DH None SHA256 Camellia(256) HIGH
AECDH-AES128-SHA ECDH None SHA1 AES(128) MEDIUM
AECDH-AES256-SHA ECDH None SHA1 AES(256) HIGH

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)

port 25 / tcp over ssl


PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Components that support SSL v2.0 or older, OR SSL v3.0/TLS with 128-bit encryption in conjunction with SSL v2.0
The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score: 3.9 E:F/RL:W/RC:C
Severity: 3 
QID: 38628
Category: General remote services
CVE ID: -
Vendor Reference: [Deprecating TLS 1.0 and TLS 1.1](#)
Bugtraq ID: -
Last Update: 2021-07-12 22:18:19.0

THREAT:

TLS is capable of using a multitude of ciphers (algorithms) to create the public and private key pairs. For example if TLSv1.0 uses either the RC4 stream cipher, or a block cipher in CBC mode. RC4 is known to have biases and the block cipher in CBC mode is vulnerable to the POODLE attack.

TLSv1.0, if configured to use the same cipher suites as SSLv3, includes a means by which a TLS implementation can downgrade the connection to SSL v3.0, thus weakening security.

[A POODLE-type](#) attack could also be launched directly at TLS without negotiating a downgrade.

This QID is an automatic PCI FAIL in accordance with the PCI standards.

Further details can be found under:

[PCI: ASV Program Guide v3.1 \(page 27\)](#)

[PCI: Use of SSL Early TLS and ASV Scans](#)

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to [Deprecating TLS 1.0 and TLS 1.1](#)

IMPACT:

An attacker can exploit cryptographic flaws to conduct man-in-the-middle type attacks or to decryption communications.

For example: An attacker could force a downgrade from the TLS protocol to the older SSLv3.0 protocol and exploit the POODLE vulnerability, read secure communications or maliciously modify messages.

[A POODLE-type](#) attack could also be launched directly at TLS without negotiating a downgrade.

SOLUTION:

Disable the use of TLSv1.0 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1 If the test is successful, then the target support TLSv1

RESULT:

TLSv1.0 is supported

SSL Certificate - Invalid Maximum Validity Date Detected

port 25 / tcp over ssl

PCI COMPLIANCE STATUS


PCI Severity Level:

MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score: 6.4 AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score: 5.2 E:U/RL:W/RC:C
Severity: 2 

QID:	38685
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-04-13 18:30:30.0

THREAT:
Subscriber Certificates issued on or after 1 September 2020 SHOULD NOT have a Validity Period greater than 397 days and MUST NOT have a Validity Period greater than 398 days. (13 months)
Subscriber Certificates issued after 1 March 2018, but prior to 1 September 2020, MUST NOT have a Validity Period greater than 825 days. (27 months)
Subscriber Certificates issued after 1 July 2016 but prior to 1 March 2018 MUST NOT have a Validity Period greater than 39 months.
SSL certificates have limited validity periods so that the certificate's holder identity information is re-authenticated more frequently.
It is detected that maximum validity of certificate on the system is more than what is recommended.

IMPACT:
By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:
Please install a server certificate with recommended maximum validity.

RESULT:
Certificate #0 CN=localhost.localdomain ISSUER:_CN=localhost.localdomain is valid for more than 398 days

HTTP Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	4.3 AV:N/AC:M/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	3.5 E:U/RL:U/RC:UR
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	11827
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-01-18 13:22:51.0

THREAT:
This QID reports the absence of the following [HTTP headers](#) according to [CWE-693: Protection Mechanism Failure](#):
X-Content-Type-Options: This HTTP header will prevent the browser from interpreting files as a different MIME type to what is specified in the Content-Type HTTP header.
Strict-Transport-Security: The HTTP Strict-Transport-Security response header (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol.

QID Detection Logic:

This unauthenticated QID looks for the presence of the following HTTP responses:

The Valid directives are as follows: X-Content-Type-Options: nosniff

Strict-Transport-Security: max-age=< [;includeSubDomains]

IMPACT:

Depending on the vulnerability being exploited, an unauthenticated remote attacker could conduct cross-site scripting, clickjacking or MIME-type sniffing attacks.

SOLUTION:

Note: To better debug the results of this QID, it is requested that customers execute commands to simulate the following functionality: curl -lkl --verbose.

CWE-693: Protection Mechanism Failure mentions the following - The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.

Customers are advised to set proper [X-Content-Type-Options](#) and [Strict-Transport-Security](#) HTTP response headers.

Depending on their server software, customers can set directives in their site configuration or Web.config files. Few examples are:

X-Content-Type-Options:

Apache: Header always set X-Content-Type-Options: nosniff

HTTP Strict-Transport-Security:

Apache: Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

Nginx: add_header Strict-Transport-Security max-age=31536000;

Note: Network devices that include a HTTP/HTTPS console for administrative/management purposes often do not include all/some of the security headers.

This is a known issue and it is recommend to contact the vendor for a solution.

RESULT:

X-Content-Type-Options HTTP Header missing on port 443.

GET / HTTP/1.1

Host: basil.wingpath.co.uk

Connection: Keep-Alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0

HTTP/1.1 200 OK

Date: Thu, 16 May 2024 11:02:18 GMT

Server: Apache/2.4.41 (Ubuntu)

Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT

ETag: "2aa6-5f040bdba30ce"

Accept-Ranges: bytes

Content-Length: 10918

Vary: Accept-Encoding

Keep-Alive: timeout=5, max=96

Connection: Keep-Alive

Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">

<!--

Modified from the Debian original for Ubuntu

Last updated: 2016-11-16

See: <https://launchpad.net/bugs/1288690>

-->

<head>

```
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Ubuntu Default Page: It works</title>
<style type="text/css" media="screen">

* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}

div.main_page {
position: relative;
display: table;

width: 800px;

margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding: 0px 0px 0px 0px;

border-width: 2px;
border-color: #212738;
border-style: solid;

background-color: #FFFFFF;

text-align: center;
}

div.page_header {
height: 99px;
width: 100%;

background-color: #F5F6F7;
}

div.page_header span {
margin: 15px 0px 0px 50px;

font-size: 180%;
font-weight: bold;
}

div.page_header img {
margin: 3px 0px 0px 40px;

border: 0px 0px 0px;
```

```
}
```

```
div.table_of_contents {  
clear: left;
```

```
min-width: 200px;
```

```
margin: 3px 3px 3px 3px;
```

```
background-color: #FFFFFF;
```

```
text-align: left;  
}
```

```
div.table_of_contents_item {  
clear: left;
```

```
width: 100%;
```

```
margin: 4px 0px 0px 0px;
```

```
background-color: #FFFFFF;
```

```
color: #000000;  
text-align: left;  
}
```

```
div.table_of_contents_item a {  
margin: 6px 0px 0px 6px;  
}
```

```
div.content_section {  
margin: 3px 3px 3px 3px;
```

```
background-color: #FFFFFF;
```

```
text-align: left;  
}
```

```
div.content_section_text {  
padding: 4px 8px 4px 8px;
```

```
color: #000000;  
font-size: 100%;  
}
```

```
div.content_section_text pre {  
margin: 8px 0px 8px 0px;  
padding: 8px 8px 8px 8px;
```

```
border-width: 1px;  
border-style: dotted;  
border-color: #000000;
```

```
background-color: #F5F6F7;
```

```
font-style: italic;
}

div.content_section_text p {
margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
padding: 4px 8px 4px 16px;
}

div.section_header {
padding: 3px 6px 3px 6px;

background-color: #8E9CB2;

color: #FFFFFF;
font-weight: bold;
font-size: 112%;
text-align: center;
}

div.section_header_red {
background-color: #CD214F;
}

div.section_header_grey {
background-color: #9F9386;
}

.floating_element {
position: relative;
float: left;
}

div.table_of_contents_item a,
div.content_section_text a {
text-decoration: none;
font-weight: bold;
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
color: #000000;
}

div.table_of_contents_item a:hover {
background-color: #000000;

color: #FFFFFF;
}

div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
```



```
background-color: #DCDFE6;

color: #000000;
}

div.content_section_text a:hover {
background-color: #000000;

color: #DCDFE6;
}

div.validator {
}
</style>
</head>
<body>
<div class="main_page">
<div class="page_header floating_element">

<span class="floating_element">
Apache2 Ubuntu Default Page
</span>
</div>
<!-- <div class="table_of_contents floating_element">
<div class="section_header section_header_grey">
TABLE OF CONTENTS
</div>
<div class="table_of_contents_item floating_element">
<a href="#about">About</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#changes">Changes</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#scope">Scope</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#files">Config files</a>
</div>
</div>
-->
<div class="content_section floating_element">

<div class="section_header section_header_red">
<div id="about"></div>
It works!
</div>
<div class="content_section_text">
<p>
This is the default welcome page used to test the correct
operation of the Apache2 server after installation on Ubuntu systems.
It is based on the equivalent page on Debian, from which the Ubuntu Apache
packaging is derived.
If you can read this page, it means that the Apache HTTP server installed at
this site is working properly. You should <b>replace this file</b> (located at
```

<tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.

</p>

<p>

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance.

If the problem persists, please contact the site's administrator.

</p>

</div>

<div class="section_header">

<div id="changes"></div>

Configuration Overview

</div>

<div class="content_section_text">

<p>

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is

fully documented in

/usr/share/doc/apache2/README.Debian.gz. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the manual if the <tt>apache2-doc</tt> package was installed on this server.

</p>

<p>

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

</p>

<pre>

/etc/apache2/

|-- apache2.conf

| `-- ports.conf

|-- mods-enabled

| |-- *.load

| `-- *.conf

|-- conf-enabled

| `-- *.conf

|-- sites-enabled

| `-- *.conf

</pre>

<tt>apache2.conf</tt> is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

<tt>ports.conf</tt> is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

Configuration files in the <tt>mods-enabled/</tt>,
<tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain
particular configuration snippets which manage modules, global configuration
fragments, or virtual host configurations, respectively.

They are activated by symlinking available
configuration files from their respective
*-available/ counterparts. These should be managed
by using our helpers

<tt>

a2enmod,

a2dismod,

</tt>

<tt>

a2ensite,

a2dissite,

</tt>

and

<tt>

a2enconf,

a2disconf

</tt>. See their respective man pages for detailed information.

The binary is called apache2. Due to the use of
environment variables, in the default configuration, apache2 needs to be
started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>.
Calling <tt>/usr/bin/apache2</tt> directly will not work with the
default configuration.

</div>

<div class="section_header">

<div id="docroot"></div>

Document Roots

</div>

<div class="content_section_text">

<p>

By default, Ubuntu does not allow access through the web browser to
any file apart of those located in <tt>/var/www/</tt>,
public_html
directories (when enabled) and <tt>/usr/share</tt> (for web
applications). If your site is using a web document root
located elsewhere (such as in <tt>/srv/</tt>) you may need to whitelist your
document root directory in <tt>/etc/apache2/apache2.conf</tt>.

</p>

<p>

The default Ubuntu document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www. This is different
to previous releases which provides better security out of the box.

```
</p>
</div>

<div class="section_header">
<div id="bugs"></div>
Reporting Problems
</div>
<div class="content_section_text">
<p>
Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
Apache2 package with Ubuntu. However, check <a
href="https://bugs.launchpad.net/ubuntu/+source/apache2"
rel="nofollow">existing bug reports</a> before reporting a new bug.
</p>
<p>
Please report bugs specific to modules (such as PHP and others)
to respective packages, not to the web server itself.
</p>
</div>
```

```
</div>
</div>
<div class="validator">
</div>
</body>
</html>
```

Strict-Transport-Security HTTP Header missing on port 443.

HTTP/1.1 200 OK
Date: Thu, 16 May 2024 11:02:18 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT
ETag: "2aa6-5f040bdba30ce"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=95
Connection: Keep-Alive
Content-Type: text/html

SSL Certificate - Self-Signed Certificate port 25 / tcp over ssl


PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	6.4 AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	4.7 E:U/RL:W/RC:UC
Severity:	2 
QID:	38169
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-23 18:38:59.0

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The client can trust that the Server Certificate belongs to the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.

By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

IMPACT:

By exploiting this vulnerability, an attacker can launch a man-in-the-middle attack.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=localhost.localdomain is a self signed certificate.

SSL Certificate - Signature Verification Failed Vulnerability

port 25 / tcp over ssl

PCI COMPLIANCE STATUS


PCI Severity Level:

MED

FAIL

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	6.4 AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	4.7 E:U/RL:W/RC:UC
Severity:	2 
QID:	38173
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-02-28 13:28:19.0

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:

If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

RESULT:

Certificate #0 CN=localhost.localdomain ISSUER:_CN=localhost.localdomain self signed certificate

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server Supports Transport Layer Security (TLSv1.1)

port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level:

LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	2.2 E:U/RL:U/RC:C
Severity:	3 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38794
Category:	General remote services
CVE ID:	-
Vendor Reference:	Deprecating TLS 1.0 and TLS 1.1
Bugtraq ID:	-
Last Update:	2022-12-07 05:51:15.0

THREAT:

The scan target supports version 1.1 of the TLS protocol. That version is in the process of being deprecated and is no longer recommended. Instead the newer versions 1.2 and/or 1.3 should be used. The TLSv1.1 protocol itself does not have any currently exploitable vulnerabilities. However some vendor implementations of TLSv1.1 have weaknesses which may be exploitable.

This QID is posted as potential, when servers require client certificates and we cannot complete the handshake.

NOTE: On March 31, 2021 Transport Layer Security (TLS) versions 1.0 (RFC 2246) and 1.1 (RFC 4346) are formally deprecated. Refer to [Deprecating TLS 1.0 and TLS 1.1](#)

IMPACT:

Supporting TLSv1.1 by itself does not necessarily have any harmful consequences, but it is no longer considered best practice because of bad past experience with some vendor implementations of TLSv1.1.

SOLUTION:

Disable the use of TLSv1.1 protocol in favor of a cryptographically stronger protocol such as TLSv1.2. The following openssl commands can be used to do a manual test: openssl s_client -connect ip:port -tls1_1 If the test is successful, then the target support TLSv1.1

RESULT:

TLSv1.1 is supported

SSL Certificate - Subject Common Name Does Not Match Server FQDN port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: Low

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	2.1 E:U/RL:W/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38170
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-10-11 16:30:02.0

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

A certificate whose Subject commonName or subjectAltName does not match the server FQDN offers only encryption without authentication.

Please note that a false positive reporting of this vulnerability is possible in the following case:

If the common name of the certificate uses a wildcard such as *.somedomainname.com and the reverse DNS resolution of the target IP is not configured. In this case there is no way for Qualys to associate the wildcard common name to the IP. Adding a reverse DNS lookup entry to the target IP will solve this problem.

IMPACT:

A man-in-the-middle attacker can exploit this vulnerability in tandem with a DNS cache poisoning attack to lure the client to another server, and then steal all the encryption communication.

SOLUTION:

Please install a server certificate whose Subject commonName or subjectAltName matches the server FQDN.

RESULT:

Certificate #0 CN=localhost.localdomain (localhost.localdomain) doesn't resolve (localhost.localdomain) doesn't resolve

AutoComplete Attribute Not Disabled for Password in Form Based Authentication port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: Low

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	2.0 E:U/RL:U/RC:UC
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	86729
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-01 13:30:46.0

THREAT:

The Web server allows form based authentication without disabling the autoComplete feature for the password field.

Autocomplete should be turned off for any input that takes sensitive information such as credit card number, CVV2/CVC code, U.S. social security number, etc.

IMPACT:

If the browser is used in a shared computing environment where more than one person may use the browser, then "autocomplete" values may be retrieved or submitted by an unauthorized user.

SOLUTION:

Contact the vendor to have the autoComplete attribute disabled for the password field in all forms. The autoComplete attribute should also be disabled for the user ID field.

Developers can add the following attribute to the form or input element: autocomplete="off"

This attribute prevents the browser from prompting the user to save the populated form values for later reuse.

Most browsers no longer honor autocomplete="off" for password input fields. These browsers include Chrome, Firefox, Microsoft Edge, IE, Opera

However, there is still an ability to turn off autocomplete through the browser and that is recommended for a shared computing environment.

Since the ability to turn autocomplete off for password inputs fields is controlled by the user it is highly recommended for application to enforce strong password rules.

RESULT:

GET /phpmyadmin/index.php HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

```
<form method="post" id="login_form" action="index.php" name="login_form" class="disableAjax login hide js-show">
<fieldset>
<legend><input type="hidden" name="set_session" value="3aileid5cgekki911sq7nujdht" />Log in<a href="/doc/html/index.html" target="documentation"></a></legend><div class="item">
<label for="input_username">Username:</label>
<input type="text" name="pma_username" id="input_username" value="" size="24" class="textfield"/>
</div>
<div class="item">
<label for="input_password">Password:</label>
<input type="password" name="pma_password" id="input_password" value="" size="24" class="textfield" />
</div> <input type="hidden" name="server" value="1" /></fieldset><fieldset class="tblFooters"><input value="Go" type="submit" id="input_go" /><input type="hidden"
name="target" value="index.php" /><input type="hidden" name="lang" value="en" /><input type="hidden" name="token" value="212e242355693f61657c21673b654e50"
/></fieldset>
</form>
```


GET /phpmyadmin/index.php?sql_debug=1 HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

GET /phpmyadmin/index.php/123 HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

OPTIONS /phpmyadmin/index.php HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

GET /phpmyadmin/ HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

GET /phpmyadmin/ HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.18) Gecko/2010020220 Firefox/3.0.18 (.NET CLR 3.5.30729)

GET /phpmyadmin/ HTTP/1.1
Connection: Keep-Alive
HOST: 185.132.38.51:443
Content-Type: text/xml; charset=UTF-8
User-Agent: () { ignored; }; echo Content-Type: text/plain ; echo ; echo ; /usr/bin/id

GET /phpmyadmin/phpinfo.php HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

GET /phpmyadmin/?name=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%27D HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

GET /phpmyadmin/?id=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%27D HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

GET /phpmyadmin/?referrer=%25%7B%28%23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCESS%29.%28%23_memberAccess%3F%28%23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%27D HTTP/1.1

23_memberAccess%3D%23dm%29%3A%28%28%23container%3D%23context%5B%27com.opensymphony.xwork2.ActionContext.container%27%5D%29.%28%23ognlUtil%3D%23container.getInstance%28%40com.opensymphony.xwork2.ognl.OgnlUtil%40class%29%29.%28%23ognlUtil.getExcludedPackageNames%28%29.clear%28%29%29.%28%23ognlUtil.getExcludedClasses%28%29.clear%28%29%29.%28%23context.setMemberAccess%28%23dm%29%29%29%29.%28%23cmd%3D%27QUALYS-STRUTS-370547%27%29.%28%23iswin%3D%28%40java.lang.System%40getProperty%28%27os.name%27%29.toLowerCase%28%29.contains%28%27win%27%29%29%29%29.%28%23cmds%3D%28%23iswin%3F%7B%27cmd.exe%27%2C%27c%27%2C%23cmd%7D%3A%7B%27bin/bash%27%2C%27-c%27%2C%23cmd%7D%29%29.%28%23p%3Dnew%20java.lang.ProcessBuilder%28%23cmds%29%29.%28%23p.redirectErrorStream%28true%29%29.%28%23process%3D%23p.start%28%29%29.%28%40org.apache.commons.io.IOUtils%40toString%28%23process.getInputStream%28%29%29%29%29%7D HTTP/1.1

Host: basil.wingpath.co.uk

Connection: Keep-Alive

get /phpmyadmin/ HTTP/1.1

Host: basil.wingpath.co.uk

Connection: Keep-Alive

SHA1 deprecated setting for SSH

port 22 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

LOW

PASS

The vulnerability is not included in the NVD.

VULNERABILITY DETAILS

CVSS Base Score:	2.6 AV:N/AC:H/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	2.1 E:U/RL:W/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38909
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2023-12-06 19:39:21.0

THREAT:

The SSH protocol (Secure Shell) is a method for secure remote login from one computer to another. The target is using deprecated SHA1 cryptographic settings to communicate.

IMPACT:

vulnerable to collision attacks, which are designed to fabricate the same hash value for different input data.each hash is supposedly unique.

SOLUTION:

Avoid using deprecated cryptographic settings.

Use best practices when configuring SSH.

Refer to [NIST Retires SHA-1 Cryptographic Algorithm \(SSH\)](#) .

Other documents to refer

[Deprecate settings listed for red hat](#)

[Key exchange](#)

[CBC Cipher](#)

Settings currently considered deprecated:

1.Key exchange algorithms:
diffie-hellman-group1-sha1, rsa1024sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, gss-gex-sha1-*, gss-group1-sha1-* and gss-group14-sha1-*.
2.MAC:
hmac-sha1, hmac-sha1-96, hmac-sha1-etm@openssh.com, hmac-sha1-96-etm@openssh.com
3.Host key:
ssh-rsa, ssh-dss, ssh-rsa-cert-v01@openssh.com, ssh-dss-cert-v01@openssh.com

RESULT:

Type Name
host key algorithm ssh-rsa
MAC hmac-sha1-etm@openssh.
com
MAC hmac-sha1

ICMP Timestamp Request

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score: 2.1 AV:L/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score: 1.7 E:U/RL:W/RC:C
Severity: 1 ■□□□□
QID: 82003
Category: TCP/IP
CVE ID: [CVE-1999-0524](#)
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-01-04 05:00:01.0

THREAT:
ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. It's principal purpose is to provide a protocol layer able to inform gateways of the inter-connectivity and accessibility of other gateways or hosts. "ping" is a well-known program for determining if a host is up or down. It uses ICMP echo packets.
ICMP timestamp packets are used to synchronize clocks between hosts. Revealing the current time on the system may facilitate attackers to mount further attacks. Since the risk is especially high on internet facing targets, this vulnerability will be flagged only by Internet scanners hosted by Qualys. Internal targets will not be flagged with this vulnerability.
Please see QID:82040 for a list of supported ICMP packet types.

IMPACT:
Unauthorized users can obtain information about your network by sending ICMP timestamp packets. For example, the internal systems clock should not be disclosed since some internal daemons use this value to calculate ID or sequence numbers (i.e., on SunOS servers).

SOLUTION:

You can filter ICMP messages of type "Timestamp" and "Timestamp Reply" at the firewall level. Some system administrators choose to filter most types of ICMP messages for various reasons. For example, they may want to protect their internal hosts from ICMP-based Denial Of Service attacks, such as the *Ping of Death* or *Smurf* attacks.

However, you should never filter **ALL** ICMP messages, as some of them ("Don't Fragment", "Destination Unreachable", "Source Quench", etc) are necessary for proper behavior of Operating System TCP/IP stacks.

It may be wiser to contact your network consultants for advice, since this issue impacts your overall network reliability and security.

RESULT:

Timestamp of host (network byte ordering): 10:09:24 GMT

Potential Vulnerabilities (61)

Apache Hypertext Transfer Protocol Server (HTTP Server) mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism
Vulnerability port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.5 E:U/RL:OF/RC:C
Severity:	5 <div></div>
QID:	730529
Category:	CGI
CVE ID:	CVE-2022-31813
Vendor Reference:	Apache HTTP Server
Bugtraq ID:	-
Last Update:	2023-12-28 13:20:48.0

THREAT:

Apache HTTP Server is an HTTP web server application.

Affected Versions:

Apache HTTP Server versions 2.4.53 and earlier

QID Detection Logic:(Unauthenticated)

This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation allows information disclosure and possible remote code execution

SOLUTION:

Customers are advised to update latest Apache httpd

For more information, visit [here](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache httpd](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 80 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Apache Hypertext Transfer Protocol Server (HTTP Server) mod_proxy X-Forwarded-For dropped by hop-by-hop mechanism

Vulnerabilityport 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.5 E:U/RL:OF/RC:C
Severity:	5 <div></div>
QID:	730529
Category:	CGI
CVE ID:	CVE-2022-31813
Vendor Reference:	Apache HTTP Server
Bugtraq ID:	-
Last Update:	2023-12-28 13:20:48.0

THREAT:

Apache HTTP Server is an HTTP web server application.

Affected Versions:

Apache HTTP Server versions 2.4.53 and earlier

QID Detection Logic:(Unauthenticated)

This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation allows information disclosure and possible remote code execution

SOLUTION:

Customers are advised to update latest Apache httpd
For more information, visit [here](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache httpd](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 443 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

PhpMyAdmin Multiple Vulnerabilities (PMASA-2020-5,PMASA-2020-6)

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

HIGH

FAIL

Automatic Failure: SQL Injection

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.9 E:POC/RL:OF/RC:C
Severity:	5 <div></div>
QID:	730123
Category:	CGI
CVE ID:	CVE-2020-26935 , CVE-2020-26934
Vendor Reference:	PMASA-2020-5 , PMASA-2020-6
Bugtraq ID:	-
Last Update:	2024-03-01 00:00:02.0

THREAT:
PhpMyAdmin is a free software tool written in PHP and intended to handle the administration of MySQL over the Internet.
CVE-2020-26935: A SQL injection vulnerability was discovered in how phpMyAdmin processes SQL statements in the search feature.
CVE-2020-26934: A vulnerability was discovered where an attacker can cause an XSS attack through the transformation feature.
Affected Versions:
phpMyAdmin versions from 4.9.x prior to 4.9.6.
phpMyAdmin versions from 5.0.x prior to 5.0.3.

QID Detection Logic (unauthenticated):
Look for vulnerable version of phpmyadmin installed.

IMPACT:
Successful exploitation allows remote attackers to inject and execute arbitrary SQL code or steal sensitive information.

SOLUTION:
Users are advised to upgrade to [phpMyAdmin 4.9.6 or 5.0.3](#) or the latest version.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[PMASA-2020-6](#)
[PMASA-2020-5](#)

RESULT:
>phpMyAdmin 4.9.5 documentation<

Apache Hypertext Transfer Protocol Server (HTTP Server) Multiple Security Vulnerabilities (CVE-2022-28330, CVE-2022-28614, CVE-2022-28615, CVE-2022-29404, CVE-2022-30556)

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	6.4 AV:N/AC:L/Au:N/C:P/I:N/A:P
CVSS Temporal Score:	4.7 E:U/RL:OF/RC:C
Severity:	5 <div></div>
QID:	731514
Category:	CGI
CVE ID:	CVE-2022-28330 , CVE-2022-28614 , CVE-2022-28615 , CVE-2022-29404 , CVE-2022-30556
Vendor Reference:	Apache http server
Bugtraq ID:	-
Last Update:	2024-05-08 18:07:45.0

THREAT:
Apache HTTP Server is an HTTP web server application.

CVE-2022-28330: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

CVE-2022-28614: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_lua's r:puts() function.

CVE-2022-28615: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer.

CVE-2022-29404: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

CVE-2022-30556: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

Affected Versions:
Apache HTTP Server versions 2.4.53 and earlier

QID Detection Logic:(Unauthenticated)
This QID checks for server banners to detect if the target is running the vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may compromise Confidentiality, Integrity, and Availability of the Data.
SOLUTION:
Customers are advised to update latest Apache httpd
For more information, visit [here](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 443 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

Apache Hypertext Transfer Protocol Server (HTTP Server) Multiple Security Vulnerabilities (CVE-2022-28330, CVE-2022-28614, CVE-2022-28615, CVE-2022-29404, CVE-2022-30556)

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	6.4 AV:N/AC:L/Au:N/C:P/I:N/A:P
CVSS Temporal Score:	4.7 E:U/RL:OF/RC:C
Severity:	5 <div></div>
QID:	731514
Category:	CGI
CVE ID:	CVE-2022-28330 , CVE-2022-28614 , CVE-2022-28615 , CVE-2022-29404 , CVE-2022-30556
Vendor Reference:	Apache http server
Bugtraq ID:	-
Last Update:	2024-05-08 18:07:45.0

THREAT:

Apache HTTP Server is an HTTP web server application.

CVE-2022-28330: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

CVE-2022-28614: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_lua's r:puts() function.

CVE-2022-28615: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer.

CVE-2022-29404: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

CVE-2022-30556: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

Affected Versions:

Apache HTTP Server versions 2.4.53 and earlier

QID Detection Logic:(Unauthenticated)

This QID checks for server banners to detect if the target is running the vulnerable version of apache httpd.

IMPACT:

Successful exploitation of this vulnerability may compromise Confidentiality, Integrity, and Availability of the Data.

SOLUTION:

Customers are advised to update latest Apache httpd

For more information, visit [here](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 80 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 282

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Apache Hypertext Transfer Protocol Server (HTTP Server) Prior to 2.4.55 Multiple Security Vulnerabilities port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	4.8 AV:A/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	3.5 E:U/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	731513
Category:	CGI
CVE ID:	CVE-2006-20001 , CVE-2022-37436
Vendor Reference:	Apache http server
Bugtraq ID:	-
Last Update:	2024-05-09 18:07:14.0

THREAT:

Apache HTTP Server is an HTTP web server application.

CVE-2006-20001: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.

CVE-2022-37436: A malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

Affected Versions:

Apache HTTP Server versions prior to 2.4.55

QID Detection Logic:(Unauthenticated)

This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation of this vulnerability may result in the breach of Confidentiality, Integrity, and Availability of data.

SOLUTION:

Customers are advised to update the latest Apache HTTP Server versions 2.4.55 or later.

For further information, please refer to [Apache HTTP Server Security Advisory](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server Security Advisory](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 443 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 309

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

The vulnerability is not scored in the NVD

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.9 E:POC/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150863
Category:	Web Application
CVE ID:	CVE-2024-24795 , CVE-2023-38709 , CVE-2024-27316
Vendor Reference:	Apache HTTP Server
Bugtraq ID:	-
Last Update:	2024-04-22 00:00:01.0

THREAT:

The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software.

Affected versions of Apache HTTP Server has multiple vulnerabilities:

HTTP response splitting (CVE-2023-38709): Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses.

HTTP Response Splitting in multiple modules (CVE-2024-24795): HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack.

HTTP/2 DoS by memory exhaustion on endless continuation frames (CVE-2024-27316): HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

Affected Versions:

Apache HTTP Server version from 2.4.0 to 2.4.58

QID Detection Logic (Unauthenticated):

This QID sends a HTTP GET request and checks the response headers to confirm if the host is running vulnerable version of Apache HTTP Server.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to the latest version of [Apache HTTP Server](#) to remediate this vulnerability. For more information related to this vulnerability please refer to [Apache's Security advisory](#)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4.59](#)

RESULT:

url: http://wingpath.co.uk/

comment: Apache HTTP Server Prior to 2.4.59 Multiple Security Vulnerabilities detected at PORT : 80

matched: HTTP/1.1 301 Moved Permanently

Date: Thu, 16 May 2024 10:24:01 GMT

Server: Apache/2.4.41 (Ubuntu)

Location: https://wingpath.co.uk/

Content-Length: 311

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://wingpath.co.uk">here</a>.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at wingpath.co.uk Port 80</address>
```

Apache HTTP Server Prior to 2.4.59 Multiple Security Vulnerabilities

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

The vulnerability is not scored in the NVD

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.9 E:POC/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150863
Category:	Web Application
CVE ID:	CVE-2024-24795 , CVE-2023-38709 , CVE-2024-27316
Vendor Reference:	Apache HTTP Server
Bugtraq ID:	-
Last Update:	2024-04-22 00:00:01.0

THREAT:

The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software.

Affected versions of Apache HTTP Server has multiple vulnerabilities:

HTTP response splitting (CVE-2023-38709): Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses.

HTTP Response Splitting in multiple modules (CVE-2024-24795): HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack.

HTTP/2 DoS by memory exhaustion on endless continuation frames (CVE-2024-27316): HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

Affected Versions:

Apache HTTP Server version from 2.4.0 to 2.4.58

QID Detection Logic (Unauthenticated):

This QID sends a HTTP GET request and checks the response headers to confirm if the host is running vulnerable version of Apache HTTP Server.

IMPACT:

Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:

Customers are advised to upgrade to the latest version of [Apache HTTP Server](#) to remediate this vulnerability. For more information related to this vulnerability please refer to [Apache's Security advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4.59](#)

RESULT:

url: https://basil.wingpath.co.uk/
comment: Apache HTTP Server Prior to 2.4.59 Multiple Security Vulnerabilities detected at PORT : 443

matched: HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:37:07 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT
ETag: "2aa6-5f040bdba30ce"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
Modified from the Debian original for Ubuntu
Last updated: 2016

Apache Hypertext Transfer Protocol (HTTP) Server Out-of-bounds Write Vulnerability

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score: 7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score: 5.5 E:U/RL:OF/RC:C
Severity: 4
QID: 730403
Category: CGI
CVE ID: CVE-2022-23943, CVE-2022-22721, CVE-2022-22720, CVE-2022-22719
Vendor Reference: Apache Security Advisory
Bugtraq ID: -
Last Update: 2023-12-28 13:20:48.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
CVE-2022-22719 - A carefully crafted request body can cause a read to a random memory area which could cause the process to crash.
CVE-2022-22720 - Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

CVE-2022-22721 - If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes.

CVE-2022-23943 - Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data.

Affected Versions:
Apache HTTP Server 2.4 - 2.4.52

IMPACT:
Successful exploitation of the vulnerability may allow an attacker to redirect victim to a malicious server.

SOLUTION:
Customers are advised to update to Apache HTTP Server 2.4.53 or later. For more information, check [Apache Security Advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache Security Advisory](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 80 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Apache Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.9 E:POC/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730209
Category:	CGI
CVE ID:	CVE-2021-34798 , CVE-2021-39275 , CVE-2021-40438
Vendor Reference:	Apache HTTP Server 2.4.49 Advisory
Bugtraq ID:	-

Last Update: 2024-05-13 00:00:01.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.

Affected Versions:

Apache HTTP Server 2.4.48 and earlier

QID Detection Logic:(Unauthenticated) This QID sends an HTTP GET request to the default page and checks for a match for a string "(Server:.*)(Apache)"; then checks for vulnerable versions of Apache HTTP.

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check [Apache Security Advisory](#)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[NA](#)

RESULT:

Vulnerable Version of Apache HTTP Server Detected on port: 443

Server: Apache/2.4.41 (Ubuntu)

Apache HTTP Server Prior to 2.4.59 Multiple Security Vulnerabilitiesport 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

The vulnerability is not scored in the NVD

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.9 E:POC/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150863
Category:	Web Application
CVE ID:	CVE-2024-24795 , CVE-2023-38709 , CVE-2024-27316
Vendor Reference:	Apache HTTP Server
Bugtraq ID:	-
Last Update:	2024-04-22 00:00:01.0

THREAT:

The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software.

Affected versions of Apache HTTP Server has multiple vulnerabilities:

HTTP response splitting (CVE-2023-38709): Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses.

HTTP Response Splitting in multiple modules (CVE-2024-24795): HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack.

HTTP/2 DoS by memory exhaustion on endless continuation frames (CVE-2024-27316): HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

Affected Versions:
Apache HTTP Server version from 2.4.0 to 2.4.58

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request and checks the response headers to confirm if the host is running vulnerable version of Apache HTTP Server.

IMPACT:
Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:
Customers are advised to upgrade to the latest version of [Apache HTTP Server](#) to remediate this vulnerability. For more information related to this vulnerability please refer to [Apache's Security advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4.59](#)

RESULT:
url: http://basil.wingpath.co.uk/
comment: Apache HTTP Server Prior to 2.4.59 Multiple Security Vulnerabilities detected at PORT : 80

```
matched: HTTP/1.1 404 Not Found
Date: Thu, 16 May 2024 10:12:13 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Apache Hypertext Transfer Protocol Server (HTTP Server) Request Smuggling Vulnerability (CVE-2022-26377)

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	5.0	AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	3.9	E:POC/RL:OF/RC:C
Severity:	4	<div><div></div><div></div><div></div><div></div><div></div></div>
QID:	731521	
Category:	CGI	

CVE ID: [CVE-2022-26377](#)
Vendor Reference: [Apache http server](#)
Bugtraq ID: -
Last Update: 2024-05-09 00:01:53.0

THREAT:
Apache HTTP Server is an HTTP web server application.
CVE-2022-26377: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to.

Affected Versions:
Apache HTTP Server versions 2.4 to 2.4.53
QID Detection Logic:(Unauthenticated)
This QID checks for server banners to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may allows an attacker to smuggle requests to the AJP server it forwards requests to.
SOLUTION:
Customers are advised to update latest Apache httpd
For more information, visit [here](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 80 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>

Apache Hypertext Transfer Protocol (HTTP) Server Out-of-bounds Write Vulnerability

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level:

HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.5 E:U/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730403
Category:	CGI
CVE ID:	CVE-2022-23943 , CVE-2022-22721 , CVE-2022-22720 , CVE-2022-22719
Vendor Reference:	Apache Security Advisory
Bugtraq ID:	-
Last Update:	2023-12-28 13:20:48.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.

CVE-2022-22719 - A carefully crafted request body can cause a read to a random memory area which could cause the process to crash.

CVE-2022-22720 - Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

CVE-2022-22721 - If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes.

CVE-2022-23943 - Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data.

Affected Versions:
Apache HTTP Server 2.4 - 2.4.52

IMPACT:
Successful exploitation of the vulnerability may allow an attacker to redirect victim to a malicious server.

SOLUTION:
Customers are advised to update to Apache HTTP Server 2.4.53 or later. For more information, check [Apache Security Advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache Security Advisory](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 443 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

Apache Hypertext Transfer Protocol Server (HTTP Server) Request Smuggling Vulnerability (CVE-2022-26377)

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	5.0 AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	3.9 E:POC/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	731521
Category:	CGI
CVE ID:	CVE-2022-26377
Vendor Reference:	Apache http server
Bugtraq ID:	-
Last Update:	2024-05-09 00:01:53.0

THREAT:

Apache HTTP Server is an HTTP web server application.

CVE-2022-26377: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to.

Affected Versions:

Apache HTTP Server versions 2.4 to 2.4.53

QID Detection Logic:(Unauthenticated)

This QID checks for server banners to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation of this vulnerability may allows an attacker to smuggle requests to the AJP server it forwards requests to.

SOLUTION:

Customers are advised to update latest Apache httpd

For more information, visit [here](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 443 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 309

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
```

```
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

Apache Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.9 E:POC/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730209
Category:	CGI
CVE ID:	CVE-2021-34798 , CVE-2021-39275 , CVE-2021-40438
Vendor Reference:	Apache HTTP Server 2.4.49 Advisory
Bugtraq ID:	-
Last Update:	2024-05-13 00:00:01.0

THREAT:
Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.

Affected Versions:
Apache HTTP Server 2.4.48 and earlier

QID Detection Logic:(Unauthenticated) This QID sends an HTTP GET request to the default page and checks for a match for a string "(Server:.*)(Apache)"; then checks for vulnerable versions of Apache HTTP.

IMPACT:
Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target.

SOLUTION:
Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check [Apache Security Advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[NA](#)

RESULT:
Vulnerable Version of Apache HTTP Server Detected on port: 80
Server: Apache/2.4.41 (Ubuntu)

Apache HTTP Server Multiple Vulnerabilities

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.5 E:U/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730109
Category:	CGI
CVE ID:	CVE-2019-17567 , CVE-2020-13938 , CVE-2020-13950 , CVE-2020-35452 , CVE-2021-26690 , CVE-2021-26691 , CVE-2021-30641
Vendor Reference:	Apache HTTP Server 2.4.48
Bugtraq ID:	-
Last Update:	2024-04-02 12:22:52.0

THREAT:

Apache HTTP Server is an HTTP web server application.

Affected Versions:

Apache HTTP Server versions prior to 2.4.46.

NOTE:

CVE-2021-26691, CVE-2021-26690, CVE-2020-35452, CVE-2020-13938 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0.
CVE-2019-17567 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6
CVE-2021-30641 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39
CVE-2020-13950 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41

QID Detection Logic:(Unauthenticated)

This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target.

SOLUTION:

Customers are advised to update Apache httpd 2.4.48.

For more information, visit [here](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4.47](#)

RESULT:

Vulnerable Version of Apache HTTP Server Detected on port: 80

Server: Apache/2.4.41 (Ubuntu)

Apache Hypertext Transfer Protocol (HTTP) Server Buffer Overflow Vulnerabilityport 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.9 E:POC/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730312
Category:	CGI
CVE ID:	CVE-2021-44790
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2023-12-28 13:20:48.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0. A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts).

Affected Versions:
Apache HTTP Server 2.4.51 and earlier

QID Detection Logic:(Unauthenticated)
This QID checks for vulnerable Apache Version by grabbing the banner from HTTP response

IMPACT:
Successful exploitation of the vulnerability may allow remote code execution and complete system compromise.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.52 or later. For more information, check [Apache Security Advisory](#)
Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache Security Advisory](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 443 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.

</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.5 E:U/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730109
Category:	CGI
CVE ID:	CVE-2019-17567 , CVE-2020-13938 , CVE-2020-13950 , CVE-2020-35452 , CVE-2021-26690 , CVE-2021-26691 , CVE-2021-30641
Vendor Reference:	Apache HTTP Server 2.4.48
Bugtraq ID:	-
Last Update:	2024-04-02 12:22:52.0

THREAT:
Apache HTTP Server is an HTTP web server application.

Affected Versions:
Apache HTTP Server versions prior to 2.4.46.

NOTE:
CVE-2021-26691, CVE-2021-26690, CVE-2020-35452, CVE-2020-13938 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0.
CVE-2019-17567 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6
CVE-2021-30641 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39
CVE-2020-13950 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41
QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.
IMPACT:
Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target.

SOLUTION:
Customers are advised to update Apache httpd 2.4.48.
For more information, visit [here](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4.47](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 80 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
```

<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>Vulnerable Version of Apache HTTP Server Detected on port: 80
Server: Apache/2.4.41 (Ubuntu)

Apache Hypertext Transfer Protocol Server (HTTP Server) Prior to 2.4.55 Multiple Security Vulnerabilities

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	4.8 AV:A/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	3.5 E:U/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	731513
Category:	CGI
CVE ID:	CVE-2006-20001 , CVE-2022-37436
Vendor Reference:	Apache http server
Bugtraq ID:	-
Last Update:	2024-05-09 18:07:14.0

THREAT:
Apache HTTP Server is an HTTP web server application.
CVE-2006-20001: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.
CVE-2022-37436: A malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

Affected Versions:
Apache HTTP Server versions prior to 2.4.55

QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may result in the breach of Confidentiality, Integrity, and Availability of data.

SOLUTION:
Customers are advised to update the latest Apache HTTP Server versions 2.4.55 or later.
For further information, please refer to [Apache HTTP Server Security Advisory](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
[Apache HTTP Server Security Advisory](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 80 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)

Content-Length: 282
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Apache Hypertext Transfer Protocol (HTTP) Server Request Smuggling Vulnerability

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	6.4 AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	5.0 E:POC/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730758
Category:	CGI
CVE ID:	CVE-2023-25690
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2024-01-16 23:00:02.0

THREAT:
Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution.

Affected Versions:
Apache HTTP Server Versions 2.4.0 through 2.4.55 (including)

QID Detection Logic(Unauthenticated):
This QID checks for vulnerable version of Apache HTTP Server by sending a GET request to a target and extracting the version from the response header.

IMPACT:
Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning.

SOLUTION:
Customers are advised to upgrade to Apache HTTP Server version 2.4.56 or later. For more information please refer to [Apache HTTP Server Security Advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:
[Apache HTTP Server Security Advisory](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 443 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

Apache Hypertext Transfer Protocol (HTTP) Server NULL Pointer Dereference and Server Side Request Forgery (SSRF)

Vulnerability

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	6.4 AV:N/AC:L/Au:N/C:N/I:P/A:P
CVSS Temporal Score:	4.7 E:U/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730313
Category:	CGI
CVE ID:	CVE-2021-44224
Vendor Reference:	Apache Security Advisory
Bugtraq ID:	-
Last Update:	2023-12-28 13:20:48.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.

A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).

Affected Versions:
Apache HTTP Server 2.4.7 - 2.4.51

QID Detection Logic:(Unauthenticated)
This QID checks for vulnerable Apache Version by grabbing the banner from HTTP response

IMPACT:

Successful exploitation of the vulnerability may allow an attacker to redirect victim to a malicious server.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.52 or later. For more information, check [Apache Security Advisory](#)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache Security Advisory](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 443 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 309

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

Apache Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.9 E:POC/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730209
Category:	CGI
CVE ID:	CVE-2021-34798 , CVE-2021-39275 , CVE-2021-40438
Vendor Reference:	Apache HTTP Server 2.4.49 Advisory
Bugtraq ID:	-
Last Update:	2024-05-13 00:00:01.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.

Affected Versions:

Apache HTTP Server 2.4.48 and earlier

QID Detection Logic:(Unauthenticated) This QID sends an HTTP GET request to the default page and checks for a match for a string "(Server:*)(Apache)"; then checks for vulnerable versions of Apache HTTP.

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check [Apache Security Advisory](#)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[NA](#)

RESULT:

Vulnerable Version of Apache HTTP Server Detected on port: 80

Server: Apache/2.4.41 (Ubuntu)

Apache Hypertext Transfer Protocol (HTTP) Server NULL Pointer Dereference and Server Side Request Forgery (SSRF) Vulnerability

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	6.4 AV:N/AC:L/Au:N/C:N/I:P/A:P
CVSS Temporal Score:	4.7 E:U/RL:OF/RC:C
Severity:	4 <div></div>
QID:	730313
Category:	CGI
CVE ID:	CVE-2021-44224
Vendor Reference:	Apache Security Advisory
Bugtraq ID:	-
Last Update:	2023-12-28 13:20:48.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.

A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).

Affected Versions:

Apache HTTP Server 2.4.7 - 2.4.51

QID Detection Logic:(Unauthenticated)

This QID checks for vulnerable Apache Version by grabbing the banner from HTTP response

IMPACT:

Successful exploitation of the vulnerability may allow an attacker to redirect victim to a malicious server.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.52 or later. For more information, check [Apache Security Advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache Security Advisory](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 80 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Apache Hypertext Transfer Protocol Server (HTTP Server) Request Smuggling Vulnerability (CVE-2022-36760)

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	1.9 AV:L/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	1.4 E:U/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	731520
Category:	CGI
CVE ID:	CVE-2022-36760
Vendor Reference:	Apache http server
Bugtraq ID:	-
Last Update:	2024-05-10 12:04:43.0

THREAT:

Apache HTTP Server is an HTTP web server application.

CVE-2022-36760: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to.

Affected Versions:
Apache HTTP Server from 2.4 through 2.4.54

QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability allows an attacker to smuggle requests to the AJP server it forwards requests.

SOLUTION:
Customers are advised to update the latest Apache HTTP Server versions 2.4.55 or later.
For further information, please refer to [Apache HTTP Server Security Advisory](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server Security Advisory](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 443 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

OpenSSH Authentication Bypass Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

FAIL

VULNERABILITY DETAILS

CVSS Base Score: 0.0 AV:L/AC:L/Au:N/C:N/I:N/A:N
CVSS Temporal Score: 0.0 E:U/RL:U/RC:C
Severity: 4 ■■■■□
QID: 38919
Category: General remote services
CVE ID: [CVE-2023-51767](#)

Vendor Reference: [OpenSSH 9.6](#)
Bugtraq ID: -
Last Update: 2024-03-29 06:08:10.0

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
In OpenSSH, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit.
Affected Versions:
OpenSSH up to version 9.6
QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.
IMPACT:
Successful exploitation allows OS command injection and row hammer attacks for authentication bypass.
SOLUTION:
There are no vendor supplied patches available at this time.
RESULT:
Vulnerable SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 detected on port 22 over TCP.

Apache Hypertext Transfer Protocol (HTTP) Server Buffer Overflow Vulnerability port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score: 7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score: 5.9 E:POC/RL:OF/RC:C
Severity: 4
QID: 730312
Category: CGI
CVE ID: [CVE-2021-44790](#)
Vendor Reference: [Apache HTTP Server Security Advisory](#)
Bugtraq ID: -
Last Update: 2023-12-28 13:20:48.0

THREAT:
Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts).
Affected Versions:
Apache HTTP Server 2.4.51 and earlier
QID Detection Logic:(Unauthenticated)
This QID checks for vulnerable Apache Version by grabbing the banner from HTTP response
IMPACT:

Successful exploitation of the vulnerability may allow remote code execution and complete system compromise.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.52 or later. For more information, check [Apache Security Advisory](#)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache Security Advisory](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 80 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 282

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Apache HTTP Server Prior to 2.4.59 Multiple Security Vulnerabilities

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

The vulnerability is not scored in the NVD

VULNERABILITY DETAILS

CVSS Base Score:	7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.9 E:POC/RL:OF/RC:C
Severity:	4 <div></div>
QID:	150863
Category:	Web Application
CVE ID:	CVE-2024-24795 , CVE-2023-38709 , CVE-2024-27316
Vendor Reference:	Apache HTTP Server
Bugtraq ID:	-
Last Update:	2024-04-22 00:00:01.0

THREAT:

The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software.

Affected versions of Apache HTTP Server has multiple vulnerabilities:

HTTP response splitting (CVE-2023-38709): Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses.

HTTP Response Splitting in multiple modules (CVE-2024-24795): HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack.

HTTP/2 DoS by memory exhaustion on endless continuation frames (CVE-2024-27316): HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion.

Affected Versions:
Apache HTTP Server version from 2.4.0 to 2.4.58

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request and checks the response headers to confirm if the host is running vulnerable version of Apache HTTP Server.

IMPACT:
Successful exploitation of this vulnerability could lead to a security breach or could affect integrity, availability, and confidentiality.

SOLUTION:
Customers are advised to upgrade to the latest version of [Apache HTTP Server](#) to remediate this vulnerability. For more information related to this vulnerability please refer to [Apache's Security advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4.59](#)

RESULT:
url: http://wingpath.co.uk/
comment: Apache HTTP Server Prior to 2.4.59 Multiple Security Vulnerabilities detected at PORT : 80

matched: HTTP/1.1 301 Moved Permanently
Date: Thu, 16 May 2024 10:36:28 GMT
Server: Apache/2.4.41 (Ubuntu)
Location: https://wingpath.co.uk/
Content-Length: 311
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://wingpath.co.uk/">here</a>.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at wingpath.co.uk Port 80</address>
```

Apache HTTP Server Multiple Vulnerabilities

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level:

HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score: 7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS Temporal Score:	5.5 E:U/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730109
Category:	CGI
CVE ID:	CVE-2019-17567 , CVE-2020-13938 , CVE-2020-13950 , CVE-2020-35452 , CVE-2021-26690 , CVE-2021-26691 , CVE-2021-30641
Vendor Reference:	Apache HTTP Server 2.4.48
Bugtraq ID:	-
Last Update:	2024-04-02 12:22:52.0

THREAT:
Apache HTTP Server is an HTTP web server application.

Affected Versions:
Apache HTTP Server versions prior to 2.4.46.

NOTE:
CVE-2021-26691, CVE-2021-26690, CVE-2020-35452, CVE-2020-13938 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0.
CVE-2019-17567 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6
CVE-2021-30641 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39
CVE-2020-13950 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41
QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target.

SOLUTION:
Customers are advised to update Apache httpd 2.4.48.
For more information, visit [here](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4.47](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 443 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	6.4 AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	5.0 E:POC/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730758
Category:	CGI
CVE ID:	CVE-2023-25690
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2024-01-16 23:00:02.0

THREAT:
Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.
Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution.

Affected Versions:
Apache HTTP Server Versions 2.4.0 through 2.4.55 (including)

QID Detection Logic(Unauthenticated):
This QID checks for vulnerable version of Apache HTTP Server by sending a GET request to a target and extracting the version from the response header.

IMPACT:
Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning.

SOLUTION:
Customers are advised to upgrade to Apache HTTP Server version 2.4.56 or later. For more information please refer to [Apache HTTP Server Security Advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server Security Advisory](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 80 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Apache HTTP Server Multiple Vulnerabilities

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	7.5	AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.5	E:U/RL:OF/RC:C
Severity:	4	<div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730109	
Category:	CGI	
CVE ID:	CVE-2019-17567 , CVE-2020-13938 , CVE-2020-13950 , CVE-2020-35452 , CVE-2021-26690 , CVE-2021-26691 , CVE-2021-30641	
Vendor Reference:	Apache HTTP Server 2.4.48	
Bugtraq ID:	-	
Last Update:	2024-04-02 12:22:52.0	

THREAT:
Apache HTTP Server is an HTTP web server application.

Affected Versions:
Apache HTTP Server versions prior to 2.4.46.

NOTE:
CVE-2021-26691, CVE-2021-26690, CVE-2020-35452, CVE-2020-13938 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.4.0.
CVE-2019-17567 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39, 2.4.38, 2.4.37, 2.4.35, 2.4.34, 2.4.33, 2.4.29, 2.4.28, 2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6
CVE-2021-30641 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41, 2.4.39
CVE-2020-13950 affects to Apache HTTP Server versions 2.4.46, 2.4.43, 2.4.41
QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may allow an attacker to execute arbitrary code on the target.

SOLUTION:
Customers are advised to update Apache httpd 2.4.48.
For more information, visit [here](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4.47](#)

RESULT:
Vulnerable Version of Apache HTTP Server Detected on port: 443
Server: Apache/2.4.41 (Ubuntu)

Apache Hypertext Transfer Protocol Server (HTTP Server) Request Smuggling Vulnerability (CVE-2022-36760)

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	1.9 AV:L/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	1.4 E:U/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	731520
Category:	CGI
CVE ID:	CVE-2022-36760
Vendor Reference:	Apache http server
Bugtraq ID:	-
Last Update:	2024-05-10 12:04:43.0

THREAT:

Apache HTTP Server is an HTTP web server application.

CVE-2022-36760: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to.

Affected Versions:

Apache HTTP Server from 2.4 through 2.4.54

QID Detection Logic:(Unauthenticated)

This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation of this vulnerability allows an attacker to smuggle requests to the AJP server it forwards requests.

SOLUTION:

Customers are advised to update the latest Apache HTTP Server versions 2.4.55 or later.

For further information, please refer to [Apache HTTP Server Security Advisory](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server Security Advisory](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 80 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 282

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

OpenSSH Command Injection Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	6.8 AV:N/AC:M/Au:N/C:P/I:P/A:P
CVSS Temporal Score:	5.3 E:POC/RL:OF/RC:C
Severity:	3 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38901
Category:	General remote services
CVE ID:	CVE-2020-15778
Vendor Reference:	openssh
Bugtraq ID:	-
Last Update:	2024-03-18 23:47:43.0

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

OpenSSH contains the following vulnerabilities:

OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

Affected Versions:

OpenSSH versions prior to 8.3

QID Detection Logic:

This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Successful exploitation allows a remote attacker for command injection in the scp.c toremote function .

SOLUTION:

Customers are advised to upgrade to [OpenSSH 8.3](#) or later to remediate these vulnerabilities.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[OpenSSH 8.3](#)

RESULT:

Vulnerable SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 detected on port 22 over TCP.

Apache Hypertext Transfer Protocol Server (HTTP Server) Multiple Security Vulnerabilities (CVE-2023-38709, CVE-2024-24795)
port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

The vulnerability is not scored in the NVD

VULNERABILITY DETAILS

CVSS Base Score:	6.4	AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score:	4.7	E:U/RL:OF/RC:C
Severity:	3	<div><div></div><div></div><div></div><div></div><div></div></div>
QID:	731355	
Category:	CGI	
CVE ID:		CVE-2023-38709 , CVE-2024-24795
Vendor Reference:		Apache http server
Bugtraq ID:	-	
Last Update:	2024-05-01 05:00:02.0	

THREAT:
Apache HTTP Server is an HTTP web server application.

CVE-2023-38709: Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses.
CVE-2024-24795: HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack.

Affected Versions:
Apache HTTP Server versions prior to 2.4.59

QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may result in the breach of Confidentiality, Integrity, and Availability of data.
SOLUTION:
Customers are advised to update the latest Apache versions respectively.
For more information, visit [here](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:
[Apache HTTP Server](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 80 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>

OpenSSH Incomplete Constrains Sensitive Information Disclosure Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	2.1 AV:L/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	1.6 E:U/RL:OF/RC:C
Severity:	3 ■ ■ ■ □ □
QID:	38928
Category:	General remote services
CVE ID:	CVE-2023-51384
Vendor Reference:	OpenSSH 9.6
Bugtraq ID:	-
Last Update:	2024-05-10 12:06:57.0

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
In ssh-agent in OpenSSH, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.

Affected Versions:
OpenSSH before version 9.6

QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:
Successful exploitation of this vulnerability leads to disclosure of sensitive information.

SOLUTION:
Customers are advised to upgrade to [OpenSSH 9.6](#) or later to remediate this vulnerability.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
[OpenSSH 9.6](#)

RESULT:
Vulnerable SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 detected on port 22 over TCP.

PhpMyAdmin Cross-Site Scripting (XSS) Vulnerability (PMASA-2023-1)port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

Automatic Failure: Cross-site Scripting (XSS) vulnerability

VULNERABILITY DETAILS

CVSS Base Score:	5.5	AV:N/AC:L/Au:S/C:P/I:P/A:N
CVSS Temporal Score:	4.1	E:U/RL:OF/RC:C
Severity:	3	<div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730737	
Category:	CGI	
CVE ID:	CVE-2023-25727	
Vendor Reference:	PMASA-2023-1	
Bugtraq ID:	-	
Last Update:	2023-03-04 10:04:52.0	

THREAT:

PhpMyAdmin is a free software tool written in PHP and intended to handle the administration of MySQL over the Internet.

An XSS vulnerability has been discovered where an authenticated user can trigger an XSS attack by uploading a specially-crafted .sql file through the drag-and-drop interface.

Affected Versions:

phpMyAdmin versions from 4.3.0 prior to 4.9.1

phpMyAdmin versions from 5.0 prior to 5.2.1

QID Detection Logic (unauthenticated):

This QID sends a HTTP GET request to "doc/html/index.html" and determines the vulnerable version of phpMyAdmin running on the target system.

IMPACT:

Successful exploitation of this vulnerability may allow an authenticated attacker to execute arbitrary JavaScript code on the target system.

SOLUTION:

Users are advised to upgrade to [phpMyAdmin 5.2.1 or 4.9.11](#) or the latest version. Workaround:

Disable the configuration directive ``$cfg[enable_drag_drop_import]``, users will be unable to use the drag and drop upload which would protect against the vulnerability.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[PMASA-2023-1](#)

RESULT:

>phpMyAdmin 4.9.5 documentation<

PhpMyAdmin Authentication Bypass Vulnerability (PMASA-2022-1)

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	4.0	AV:N/AC:L/Au:S/C:N/I:P/A:N
CVSS Temporal Score:	3.0	E:U/RL:OF/RC:C
Severity:	3	<div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730339	
Category:	CGI	

CVE ID: [CVE-2022-23807](#)
Vendor Reference: [PMASA-2022-1](#)
Bugtraq ID: -
Last Update: 2022-02-07 13:03:29.0

THREAT:
PhpMyAdmin is a free software tool written in PHP and intended to handle the administration of MySQL over the Internet.
CVE-2022-23807: A valid user who is already authenticated to phpMyAdmin can manipulate their account to bypass two-factor authentication for future login instances.
Affected Versions:
phpMyAdmin versions from 4.9.x prior to 4.9.8.
phpMyAdmin versions from 5.1.x prior to 5.1.2.
QID Detection Logic (unauthenticated):
Look for vulnerable version of phpmyadmin installed.
IMPACT:
Successful exploitation of this vulnerability may allow an authenticated user to manipulate and bypass two-factor authentication for future login instances.
SOLUTION:
Users are advised to upgrade to [phpMyAdmin 4.9.8 or 5.1.2](#) or the latest version.
Patch:
Following are links for downloading patches to fix the vulnerabilities:

[PMASA-2022-1](#)

RESULT:
>phpMyAdmin 4.9.5 documentation<

Apache Hypertext Transfer Protocol Server (HTTP Server) Multiple Security Vulnerabilities (CVE-2023-38709, CVE-2024-24795)
port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL The vulnerability is not scored in the NVD

VULNERABILITY DETAILS

CVSS Base Score: 6.4 AV:N/AC:L/Au:N/C:P/I:P/A:N
CVSS Temporal Score: 4.7 E:U/RL:OF/RC:C
Severity: 3 ■ ■ ■ ■ ■
QID: 731355
Category: CGI
CVE ID: [CVE-2023-38709](#), [CVE-2024-24795](#)
Vendor Reference: [Apache http server](#)
Bugtraq ID: -
Last Update: 2024-05-01 05:00:02.0

THREAT:
Apache HTTP Server is an HTTP web server application.

CVE-2023-38709: Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses.
CVE-2024-24795: HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack.

Affected Versions:
Apache HTTP Server versions prior to 2.4.59

QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may result in the breach of Confidentiality, Integrity, and Availability of data.

SOLUTION:
Customers are advised to update the latest Apache versions respectively.
For more information, visit [here](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server](#)

RESULT:
Vulnerable Apache HTTP Server detected on port 443 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.

</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>

PhpMyAdmin Information Disclosure Vulnerability

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score: 5.0 AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Score: 3.7 E:U/RL:OF/RC:C
Severity: 3
QID: 730632
Category: CGI

CVE ID: [CVE-2022-0813](#)
Vendor Reference: [phpMyAdmin Release Note](#)
Bugtraq ID: -
Last Update: 2022-11-02 14:10:48.0

THREAT:

PhpMyAdmin is a free software tool written in PHP and intended to handle the administration of MySQL over the Internet.

CVE-2022-0813: PhpMyAdmin 5.1.1 and before allows an attacker to retrieve potentially sensitive information by creating invalid requests. This affects the lang parameter, the pma_parameter, and the cookie section.

Affected Versions:

PhpMyAdmin version 5.1.1 and before.

QID Detection Logic (unauthenticated):

This QID sends a HTTP GET request to "doc/html/index.html" and determines the vulnerable version of phpMyAdmin running on the target system.

IMPACT:

Successful exploitation of this vulnerability may allow an attacker to retrieve potentially sensitive information by creating invalid requests.

SOLUTION:

Users are advised to upgrade to [phpMyAdmin 5.1.3](#) or the latest version.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[phpMyAdmin Release Note](#)

RESULT:

>phpMyAdmin 4.9.5 documentation<

Apache HTTP Server multiple vulnerabilities

port 443 / tcp over ssl


PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score: **5.8** AV:N/AC:M/Au:N/C:P/I:P/A:N
CVSS Temporal Score: **4.3** E:U/RL:OF/RC:C
Severity: **3** 
QID: 13745
Category: CGI
CVE ID: [CVE-2020-1934](#), [CVE-2020-1927](#)
Vendor Reference: [Apache HTTP Server](#)
Bugtraq ID: -
Last Update: 2021-11-29 13:36:39.0

THREAT:

Apache HTTP Server is an HTTP web server application.

CVE-2020-1934: In Apache HTTP Server, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

CVE-2020-1927: In Apache HTTP Server, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

Affected Versions:

Apache httpd 2.4.0 to 2.4.41

QID Detection Logic:(Unauthenticated)

This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

This vulnerability could be exploited to gain partial access to sensitive information. Malicious users could also use this vulnerability to change partial contents or configuration on the system

SOLUTION:

Customers are advised to update Apache httpd to 2.4.42 or later.

For more information, visit [here](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache httpd 2.4.42 or later 2.4.](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 443 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 309

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

OpenSSH Man-in-the-Middle (MITM) Attack Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	3.2 E:U/RL:OF/RC:C
Severity:	3 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38902
Category:	General remote services

CVE ID: [CVE-2020-14145](#)
Vendor Reference: [CVE-2020-14145](#)
Bugtraq ID: -
Last Update: 2023-11-27 13:23:22.0

THREAT:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.
OpenSSH contains the following vulnerabilities:
CVE-2020-14145: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.
Affected Versions:
OpenSSH 5.7-8.6

QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:
Successful exploitation allows man-in-the-middle attackers to target initial connection attempts
SOLUTION:
Customers are advised to upgrade to [OpenSSH 8.7](#) or later to remediate these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
[CVE-2020-14145](#)

RESULT:
Vulnerable SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 detected on port 22 over TCP.


OpenSSH OS Command Injection Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score: 7.5 AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS Temporal Score: 5.9 E:POC/RL:OF/RC:C
Severity: 3 
QID: 38915
Category: General remote services
CVE ID: [CVE-2023-51385](#)
Vendor Reference: [OpenSSH 9.6](#)
Bugtraq ID: -
Last Update: 2024-02-23 11:41:49.0

THREAT:
OpenSSH is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

In OpenSSH, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations.

Affected Versions:

OpenSSH before version 9.6

QID Detection Logic:

This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:

Successful exploitation allows attacker is able to manipulate input data in such a way that it is executed as a command by the operating system using OS command injection.

SOLUTION:

Customers are advised to upgrade to [OpenSSH 9.6](#) or later to remediate this vulnerability.

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[OpenSSH 9.6](#)

RESULT:

Vulnerable SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 detected on port 22 over TCP.

Apache HTTP Server multiple vulnerabilities

port 80 / tcp


PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score: **5.8** AV:N/AC:M/Au:N/C:P/I:P/A:N
CVSS Temporal Score: **4.3** E:U/RL:OF/RC:C
Severity: **3** 
QID: 13745
Category: CGI
CVE ID: [CVE-2020-1934](#), [CVE-2020-1927](#)
Vendor Reference: [Apache HTTP Server](#)
Bugtraq ID: -
Last Update: 2021-11-29 13:36:39.0

THREAT:

Apache HTTP Server is an HTTP web server application.

CVE-2020-1934: In Apache HTTP Server, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

CVE-2020-1927: In Apache HTTP Server, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

Affected Versions:

Apache httpd 2.4.0 to 2.4.41

QID Detection Logic:(Unauthenticated)

This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

This vulnerability could be exploited to gain partial access to sensitive information. Malicious users could also use this vulnerability to change partial contents or configuration on the system

SOLUTION:

Customers are advised to update Apache httpd to 2.4.42 or later.
For more information, visit [here](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache httpd 2.4.42 or later 2.4.](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 80 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 282

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Possible Mail Relay

port 25 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: HIGH

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	10 AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS Temporal Score:	9 E:F/RL:W/RC:C
Severity:	3 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	74037
Category:	Mail services
CVE ID:	CVE-1999-0512 , CVE-2002-1278 , CVE-2003-0285
Vendor Reference:	-
Bugtraq ID:	7580 , 6118
Last Update:	2013-10-23 21:45:50.0

THREAT:

The Internet Electronic Mail exchange protocol (SMTP) is designed to work with relays. These days, there is less of a need for relaying functions and, in fact, relaying

functions are highly vulnerable to attacks because they allow unauthorized users to connect once to a mail server for a single message. Then, the relaying server distributes the message to thousands of recipients.

It is possible that mail relaying is allowed by the mail server on the host. More details about the specific relaying addresses that are accepted by the mail server are given in the Results section. Since a mail server that accepts a relaying address may be configured not to actually deliver the mail to that address. If this is the case, you may safely ignore this report.

IMPACT:

If mail relaying is indeed allowed, unauthorized Internet users can exploit your Mail server to send anonymous e-mail messages, send massive advertisement messages to unwilling recipients, consume bandwidth or cause denial of service on your servers.

SOLUTION:

Disallow mail relaying if it is allowed. The mail exchanger will need to be reconfigured accordingly.

RESULT:

HELO qualysguard.com

250 basil.wingpath.co.uk

MAIL FROM:<qgmrfom@basil.wingpath.co.uk>

250 2.1.0 Ok

RCPT TO:<@qualysguard.com:qgmrttest@basil.wingpath.co.uk>

250 2.1.5 Ok

DATA

354 End data with <CR><LF>.<CR><LF>

QG mail relay test # 6

.

250 2.0.0 Ok: queued as C7A5915F2AF

Apache Hypertext Transfer Protocol Server (HTTP Server) HTTP/2 Method Injection Vulnerability

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	5.0 AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	3.9 E:POC/RL:OF/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730210
Category:	CGI
CVE ID:	CVE-2021-33193
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2024-03-01 00:00:02.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.

A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning.

Affected Versions:

Apache HTTP Server 2.4.17 to 2.4.48.

QID Detection Logic:(Unauthenticated)

This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation of this vulnerability may allow request splitting or cache poisoning.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check [Apache Security Advisory](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[NA](#)

RESULT:

Vulnerable Version of Apache HTTP Server Detected on port: 80

Server: Apache/2.4.41 (Ubuntu)

Apache Hypertext Transfer Protocol Server (HTTP Server) HTTP/2 Method Injection Vulnerability

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	5.0 AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	3.9 E:POC/RL:OF/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730210
Category:	CGI
CVE ID:	CVE-2021-33193
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2024-03-01 00:00:02.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.

A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning.

Affected Versions:

Apache HTTP Server 2.4.17 to 2.4.48.

QID Detection Logic:(Unauthenticated)

This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation of this vulnerability may allow request splitting or cache poisoning.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check [Apache Security Advisory](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

NA

RESULT:

Vulnerable Version of Apache HTTP Server Detected on port: 443

Server: Apache/2.4.41 (Ubuntu)

Apache Hypertext Transfer Protocol Server (HTTP Server) HTTP/2 Method Injection Vulnerability port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	5.0 AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	3.9 E:POC/RL:OF/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730210
Category:	CGI
CVE ID:	CVE-2021-33193
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2024-03-01 00:00:02.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.

A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning.

Affected Versions:

Apache HTTP Server 2.4.17 to 2.4.48.

QID Detection Logic:(Unauthenticated)

This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation of this vulnerability may allow request splitting or cache poisoning.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check [Apache Security Advisory](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

NA

RESULT:

Vulnerable Apache HTTP Server detected on port 443 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 309

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

OpenSSH Probable User Enumeration Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	4.3 AV:N/AC:M/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	3.4 E:POC/RL:OF/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38903
Category:	General remote services
CVE ID:	CVE-2016-20012
Vendor Reference:	OpenSSH 8.8
Bugtraq ID:	-
Last Update:	2024-03-01 00:00:02.0

THREAT:

OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

OpenSSH contains the following vulnerabilities:

CVE-2016-20012: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.

Affected Versions:
OpenSSH versions prior to 8.8

QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:
Successful exploitation allows a remote attacker to test and confirm if a certain combination of username and public key is known to an SSH server.

SOLUTION:
Customers are advised to upgrade to [OpenSSH 8.8](#) or later to remediate these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[OpenSSH 8.8 or later](#)

RESULT:
Vulnerable SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 detected on port 22 over TCP.

Apache Hypertext Transfer Protocol Server (HTTP Server) HTTP/2 Method Injection Vulnerability

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	5.0 AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	3.9 E:POC/RL:OF/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730210
Category:	CGI
CVE ID:	CVE-2021-33193
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2024-03-01 00:00:02.0

THREAT:
Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning.

Affected Versions:
Apache HTTP Server 2.4.17 to 2.4.48.

QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may allow request splitting or cache poisoning.

SOLUTION:
Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check [Apache Security Advisory](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

NA

RESULT:

Vulnerable Apache HTTP Server detected on port 80 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>Vulnerable Version of Apache HTTP Server Detected on port: 80
Server: Apache/2.4.41 (Ubuntu)
```

Apache Hypertext Transfer Protocol Server (HTTP Server) HTTP/2 Method Injection Vulnerability

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

FAIL

VULNERABILITY DETAILS

CVSS Base Score:	5.0 AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS Temporal Score:	3.9 E:POC/RL:OF/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730210
Category:	CGI
CVE ID:	CVE-2021-33193
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2024-03-01 00:00:02.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.

A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning.

Affected Versions:
Apache HTTP Server 2.4.17 to 2.4.48.

QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache http.

IMPACT:
Successful exploitation of this vulnerability may allow request splitting or cache poisoning.

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check [Apache Security Advisory](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

NA

RESULT:

Vulnerable Version of Apache HTTP Server Detected on port: 443

Server: Apache/2.4.41 (Ubuntu)

Apache Hypertext Transfer Protocol Server (HTTP Server) Prior to 2.4.58 Multiple Security Vulnerabilities

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

LOW

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	1.7 AV:L/AC:L/Au:S/C:N/I:P/A:N
CVSS Temporal Score:	1.3 E:U/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	731517
Category:	CGI
CVE ID:	CVE-2023-31122 , CVE-2023-45802
Vendor Reference:	Apache http server
Bugtraq ID:	-
Last Update:	2024-05-09 18:07:14.0

THREAT:

Apache HTTP Server is an HTTP web server application.

CVE-2023-31122: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server

CVE-2023-45802: A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.

Affected Versions:

Apache HTTP Server versions prior to 2.4.58

QID Detection Logic:(Unauthenticated)

This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation of this vulnerability may result in the breach of Confidentiality, Integrity, and Availability of data.

SOLUTION:

Customers are advised to update the latest Apache HTTP Server versions 2.4.58 or later.

For further information, please refer to [Apache HTTP Server Security Advisory](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server Security Advisory](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 80 -

Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Apache Hypertext Transfer Protocol Server (HTTP Server) Prior to 2.4.58 Multiple Security Vulnerabilities port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	1.7 AV:L/AC:L/Au:S/C:N/I:P/A:N
CVSS Temporal Score:	1.3 E:U/RL:OF/RC:C
Severity:	4 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	731517
Category:	CGI
CVE ID:	CVE-2023-31122 , CVE-2023-45802
Vendor Reference:	Apache http server
Bugtraq ID:	-
Last Update:	2024-05-09 18:07:14.0

THREAT:
Apache HTTP Server is an HTTP web server application.

CVE-2023-31122: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server

CVE-2023-45802: A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.

Affected Versions:
Apache HTTP Server versions prior to 2.4.58

QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may result in the breach of Confidentiality, Integrity, and Availability of data.

SOLUTION:

Customers are advised to update the latest Apache HTTP Server versions 2.4.58 or later.
For further information, please refer to [Apache HTTP Server Security Advisory](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server Security Advisory](#)

RESULT:

Vulnerable Apache HTTP Server detected on port 443 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

Apache HTTP Server Prior to 2.4.58 Multiple Security Vulnerabilities

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	6.4 AV:N/AC:L/Au:N/C:P/I:N/A:P
CVSS Temporal Score:	4.7 E:U/RL:OF/RC:C
Severity:	3 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150737
Category:	Web Application
CVE ID:	CVE-2023-43622 , CVE-2023-31122 , CVE-2023-45802
Vendor Reference:	Apache HTTP Server 2.4 vulnerabilities
Bugtraq ID:	-
Last Update:	2024-04-05 12:25:42.0

THREAT:

The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software.
Affected versions of Apache HTTP Server has multiple vulnerabilities:
CVE-2023-31122 : Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server

CVE-2023-43622 : DoS in HTTP/2 with initial windows size 0
CVE-2023-45802 : When a HTTP/2 stream was reset (RST frame) by a client, there was a time window where the requests memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.

Affected Versions:
Apache HTTP Server version from 2.4.0 to 2.4.57

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request and checks the response headers to confirm if the host is running vulnerable version of Apache HTTP Server.

IMPACT:
Exploitation of the vulnerability could lead to uncontrolled resource consumption or buffer over-read.

SOLUTION:
Customers are advised to upgrade to the latest version of [Apache HTTP Server](#) to remediate this vulnerability. For more information related to this vulnerability please refer to [Apache's Security advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4 vulnerabilities](#)
[Apache HTTP Server](#)

RESULT:
url: http://wingpath.co.uk/
comment: Apache HTTP Server Prior to 2.4.58 Multiple Security Vulnerabilities detected at PORT : 80

matched: HTTP/1.1 301 Moved Permanently
Date: Thu, 16 May 2024 10:31:34 GMT
Server: Apache/2.4.41 (Ubuntu)
Location: https://wingpath.co.uk/
Content-Length: 311
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://wingpath.co.uk/">here</a>.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at wingpath.co.uk Port 80</address>
```

Apache HTTP Server Prior to 2.4.58 Multiple Security Vulnerabilities

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score: 6.4 AV:N/AC:L/Au:N/C:P/I:N/A:P
CVSS Temporal Score: 4.7 E:U/RL:OF/RC:C
Severity: 3

QID: 150737
Category: Web Application
CVE ID: [CVE-2023-43622](#), [CVE-2023-31122](#), [CVE-2023-45802](#)
Vendor Reference: [Apache HTTP Server 2.4 vulnerabilities](#)
Bugtraq ID: -
Last Update: 2024-04-05 12:25:42.0

THREAT:

The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software.

Affected versions of Apache HTTP Server has multiple vulnerabilities:

CVE-2023-31122 : Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server

CVE-2023-43622 : DoS in HTTP/2 with initial windows size 0

CVE-2023-45802 : When a HTTP/2 stream was reset (RST frame) by a client, there was a time window where the requests memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.

Affected Versions:
Apache HTTP Server version from 2.4.0 to 2.4.57

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request and checks the response headers to confirm if the host is running vulnerable version of Apache HTTP Server.

IMPACT:
Exploitation of the vulnerability could lead to uncontrolled resource consumption or buffer over-read.

SOLUTION:
Customers are advised to upgrade to the latest version of [Apache HTTP Server](#) to remediate this vulnerability. For more information related to this vulnerability please refer to [Apache's Security advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4 vulnerabilities](#)
[Apache HTTP Server](#)

RESULT:
url: <https://wingpath.co.uk/modbus/>
comment: Apache HTTP Server Prior to 2.4.58 Multiple Security Vulnerabilities detected at PORT : 443

matched: HTTP/1.1 301 Moved Permanently
Date: Thu, 16 May 2024 10:19:04 GMT
Server: Apache/2.4.41 (Ubuntu)
Location: <https://wingpath.co.uk/modbus/modbus.php>
Content-Length: 329
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://wingpath.co.uk/modbus/modbus.php">here</a>.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at
```

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	6.4	AV:N/AC:L/Au:N/C:P/I:N/A:P
CVSS Temporal Score:	4.7	E:U/RL:OF/RC:C
Severity:	3	<div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150737	
Category:	Web Application	
CVE ID:	CVE-2023-43622 , CVE-2023-31122 , CVE-2023-45802	
Vendor Reference:	Apache HTTP Server 2.4 vulnerabilities	
Bugtraq ID:	-	
Last Update:	2024-04-05 12:25:42.0	

THREAT:

The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software.

Affected versions of Apache HTTP Server has multiple vulnerabilities:

CVE-2023-31122 : Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server

CVE-2023-43622 : DoS in HTTP/2 with initial windows size 0

CVE-2023-45802 : When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the requests memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.

Affected Versions:

Apache HTTP Server version from 2.4.0 to 2.4.57

QID Detection Logic (Unauthenticated):

This QID sends a HTTP GET request and checks the response headers to confirm if the host is running vulnerable version of Apache HTTP Server.

IMPACT:

Exploitation of the vulnerability could lead to uncontrolled resource consumption or buffer over-read.

SOLUTION:

Customers are advised to upgrade to the latest version of [Apache HTTP Server](#) to remediate this vulnerability. For more information related to this vulnerability please refer to [Apache's Security advisory](#)

Patch:

Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4 vulnerabilities](#)

[Apache HTTP Server](#)

RESULT:

url: https://basil.wingpath.co.uk/

comment: Apache HTTP Server Prior to 2.4.58 Multiple Security Vulnerabilities detected at PORT : 443

matched: HTTP/1.1 200 OK

Date: Thu, 16 May 2024 10:37:06 GMT

Server: Apache/2.4.41 (Ubuntu)

Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT

ETag: "2aa6-5f040bdba30ce"

Accept-Ranges: bytes

Content-Length: 10918

Vary: Accept-Encoding
Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
Modified from the Debian original for Ubuntu
Last updated: 2016
```

Apache HTTP Server Prior to 2.4.58 Multiple Security Vulnerabilities

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	6.4 AV:N/AC:L/Au:N/C:P/I:N/A:P
CVSS Temporal Score:	4.7 E:U/RL:OF/RC:C
Severity:	3 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150737
Category:	Web Application
CVE ID:	CVE-2023-43622 , CVE-2023-31122 , CVE-2023-45802
Vendor Reference:	Apache HTTP Server 2.4 vulnerabilities
Bugtraq ID:	-
Last Update:	2024-04-05 12:25:42.0

THREAT:
The Apache HTTP Server, colloquially called Apache, is a free and open-source cross-platform web server software.

Affected versions of Apache HTTP Server has multiple vulnerabilities:
CVE-2023-31122 : Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server
CVE-2023-43622 : DoS in HTTP/2 with initial windows size 0
CVE-2023-45802 : When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the requests memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.

Affected Versions:
Apache HTTP Server version from 2.4.0 to 2.4.57

QID Detection Logic (Unauthenticated):
This QID sends a HTTP GET request and checks the response headers to confirm if the host is running vulnerable version of Apache HTTP Server.

IMPACT:
Exploitation of the vulnerability could lead to uncontrolled resource consumption or buffer over-read.

SOLUTION:
Customers are advised to upgrade to the latest version of [Apache HTTP Server](#) to remediate this vulnerability. For more information related to this vulnerability please refer to [Apache's Security advisory](#)

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[Apache HTTP Server 2.4 vulnerabilities](#)

[Apache HTTP Server](#)

RESULT:

url: http://basil.wingpath.co.uk/
comment: Apache HTTP Server Prior to 2.4.58 Multiple Security Vulnerabilities detected at PORT : 80

matched: HTTP/1.1 404 Not Found
Date: Thu, 16 May 2024 10:12:12 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Apache Hypertext Transfer Protocol Server (HTTP Server) Denial of Service (DoS) Vulnerability

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Temporal Score:	3.7 E:U/RL:OF/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730211
Category:	CGI
CVE ID:	CVE-2021-36160
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2023-12-28 13:20:48.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.

A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS).

Affected Versions:
Apache HTTP Server versions 2.4.30 to 2.4.48.

QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:

Successful exploitation of this vulnerability may cause Denial of Service (DoS)

SOLUTION:

Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check [Apache Security Advisory](#).

Patch:

Following are links for downloading patches to fix the vulnerabilities:

NA

RESULT:

Vulnerable Apache HTTP Server detected on port 80 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 282

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>Vulnerable Version of Apache HTTP Server Detected on port: 80
Server: Apache/2.4.41 (Ubuntu)
```

Apache Hypertext Transfer Protocol Server (HTTP Server) Denial of Service (DoS) Vulnerability

port 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Temporal Score:	3.7 E:U/RL:OF/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730211
Category:	CGI
CVE ID:	CVE-2021-36160
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2023-12-28 13:20:48.0

THREAT:

Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS).

Affected Versions:
Apache HTTP Server versions 2.4.30 to 2.4.48.

QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may cause Denial of Service (DoS)

SOLUTION:
Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check [Apache Security Advisory](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[NA](#)

RESULT:
Vulnerable Version of Apache HTTP Server Detected on port: 443
Server: Apache/2.4.41 (Ubuntu)

Apache Hypertext Transfer Protocol Server (HTTP Server) Denial of Service (DoS) Vulnerability

port 80 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level:

MED

PASS

The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Temporal Score:	3.7 E:U/RL:OF/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	730211
Category:	CGI
CVE ID:	CVE-2021-36160
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2023-12-28 13:20:48.0

THREAT:
Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS).

Affected Versions:
Apache HTTP Server versions 2.4.30 to 2.4.48.

QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may cause Denial of Service (DoS)

SOLUTION:
Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check [Apache Security Advisory](#).

Patch:
Following are links for downloading patches to fix the vulnerabilities:

NA

RESULT:
Vulnerable Version of Apache HTTP Server Detected on port: 80
Server: Apache/2.4.41 (Ubuntu)

Apache Hypertext Transfer Protocol Server (HTTP Server) Denial of Service (DoS) Vulnerability port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASS The vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score: 5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Temporal Score: 3.7 E:U/RL:OF/RC:C
Severity: 2
QID: 730211
Category: CGI
CVE ID: CVE-2021-36160
Vendor Reference: Apache HTTP Server Security Advisory
Bugtraq ID: -
Last Update: 2023-12-28 13:20:48.0

THREAT:
Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS).
Affected Versions:
Apache HTTP Server versions 2.4.30 to 2.4.48.

QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may cause Denial of Service (DoS)
SOLUTION:
Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check Apache Security Advisory.

Patch:
Following are links for downloading patches to fix the vulnerabilities:

NA

RESULT:
Vulnerable Apache HTTP Server detected on port 443 -
Date: Thu, 16 May 2024 10:12:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 309
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">

```
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

OpenSSH Public-Key Authentication Vulnerability

PCI COMPLIANCE STATUS

PCI Severity Level: LOW

PASS

VULNERABILITY DETAILS

CVSS Base Score:	2.6 AV:N/AC:H/Au:N/C:P/I:N/A:N
CVSS Temporal Score:	1.9 E:U/RL:OF/RC:C
Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38900
Category:	General remote services
CVE ID:	CVE-2021-36368
Vendor Reference:	OpenSSH 8.9
Bugtraq ID:	-
Last Update:	2023-11-16 13:24:28.0

THREAT:
OpenSSH (OpenBSD Secure Shell) is a set of computer programs providing encrypted communication sessions over a computer network using the SSH protocol.

OpenSSH contains the following vulnerabilities:
CVE-2021-36368: If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf.

Affected Versions:
OpenSSH versions prior to 8.9

QID Detection Logic:
This unauthenticated detection works by reviewing the version of the OpenSSH service.

IMPACT:
Successful exploitation allows a remote attacker silently modify the server to support the None authentication option when a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose.

SOLUTION:
Customers are advised to upgrade to [OpenSSH 8.9](#) or later to remediate these vulnerabilities.

Patch:
Following are links for downloading patches to fix the vulnerabilities:
[OpenSSH 8.9 or later](#)

RESULT:
Vulnerable SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 detected on port 22 over TCP.

Apache Hypertext Transfer Protocol Server (HTTP Server) Denial of Service (DoS) Vulnerabilityport 443 / tcp

PCI COMPLIANCE STATUS

PCI Severity Level: MED

PASSThe vulnerability is purely a denial-of-service (DoS) vulnerability.

VULNERABILITY DETAILS

CVSS Base Score:	5.0 AV:N/AC:L/Au:N/C:N/I:N/A:P
CVSS Temporal Score:	3.7 E:U/RL:OF/RC:C
Severity:	2
QID:	730211
Category:	CGI
CVE ID:	CVE-2021-36160
Vendor Reference:	Apache HTTP Server Security Advisory
Bugtraq ID:	-
Last Update:	2023-12-28 13:20:48.0

THREAT:
Apache HTTP Server is a free and open-source cross-platform web server software, released under the terms of Apache License 2.0.
A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS).
Affected Versions:
Apache HTTP Server versions 2.4.30 to 2.4.48.
QID Detection Logic:(Unauthenticated)
This QID checks for server banner to detect if the target is running vulnerable version of apache httpd.

IMPACT:
Successful exploitation of this vulnerability may cause Denial of Service (DoS)
SOLUTION:
Customers are advised to update to Apache HTTP Server 2.4.49 or later. For more information, check Apache Security Advisory.
Patch:
Following are links for downloading patches to fix the vulnerabilities:

NA

RESULT:
Vulnerable Version of Apache HTTP Server Detected on port: 443
Server: Apache/2.4.41 (Ubuntu)

Information Gathered (90)

Default Web Page for Apache Web Server Foundport 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150842
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-03-20 03:05:30.0

THREAT:

Web server default page are common generic pages, including documentation and allow access to common configuration paths.

QID Detection Logic:

This QID checks for the web server by sending a GET request and checking the response body.

QID identifies Apache Web Server Default pages.

IMPACT:

When common default pages are exposed, version information about servers can be revealed. Attackers use this information to identify any known weaknesses and exploit.

SOLUTION:

- Create custom default pages.
- Disable or remove known/default web pages.

RESULT:

Request: <https://basil.wingpath.co.uk/>
Matched Text: >
<!--
Modified from the Debian original for Ubuntu
Last updated: 2016-11-16
See: <https://launchpad.net/bugs/1288690>
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Ubuntu Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-s
Comment: Default Web Page for Apache Web Server Found on PORT : 443

Content-Security-Policy HTTP Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	48001
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Content-Security-Policy
Bugtraq ID:	-
Last Update:	2019-03-11 17:50:46.0

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Content-Security-Policy HTTP Header missing on port 443.
GET / HTTP/1.1
Host: wingpath.co.uk
Connection: Keep-Alive

Remote Access or Management Service Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2023-09-19 12:21:48.0

THREAT:
A remote access or remote management service was detected. If such a service is accessible to malicious users it can be used to carry different type of attacks. Malicious users could try to brute force credentials or collect additional information on the service which could enable them in crafting further attacks.

The Results section includes information on the remote access service that was found on the target.

Services like Telnet, Rlogin, SSH, windows remote desktop, pcAnywhere, Citrix Management Console, Remote Admin (RAdmin), VNC, OPENVPN and ISAKMP are checked.

IMPACT:
Consequences vary by the type of attack.

SOLUTION:
Expose the remote access or remote management services only to the system administrators or intended users of the system.

RESULT:
Service name: SSH on TCP port 22.

DEFLATE Data Compression Algorithm Used for HTTPS

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	3 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	42416
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2013-08-10 00:02:05.0

THREAT:
HTTP data is compressed before it is sent from the server. DEFLATE data compression algorithm uses the LZ77 algorithm which takes advantage of repeated strings to more efficiently compress output.

DEFLATE data compression algorithm is prone to be unsafe as described in the BREACH attack. If an attacker can inject a string into a HTTPS response intended to match another unknown string (the target secret), they can iteratively guess the secret value by monitoring the compressed size of the responses for different guesses. Note: The attacker needs the capability of reading responses received by the user's browser and the capability of cause the victim to send requests from their browser to perform BREACH attack.

This QID detects that the remote HTTP server is using a gzip or DEFLATE (zlib) compression format which is using DEFLATE data compression algorithm.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:39:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT
ETag: "2aa6-5f040bdba30ce-gzip"

Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3138
Content-Type: text/html

_1F_8B_08_00_00_00_00_00_03_BDZ_EBs_DB6_12_FF_EE_BF_02U_A7_D3\$'_91_96_93_BA_B2"&_F1c_D2_99_A4_F1\$ _CA_DD_F5_93_0F"!
c_88_E0_01_A0d5_ED_FF~_BB_00H_F1%_CA_C95_D5_C4_91H_02_FB_C2_EEo_1F_D2_D1_E4_BB_AB_F7_97_D3_DFn_AF_C9_D2_AC_04_B9_FD_F4_FA_ED
/_97_A47_08_C3_7F=_BF_0C_C3_AB_E9_15_F9_F7_9B_E9_BB_B7d_18_1C_93_A9_A2_89_E6_86_CB_84_8A0_BC_FE_B5GzKc_D2q_18n6_9B`_F3<_90j_11N?
_84_0FHk_88_9B_FD_C7_81)_ED_0Cb_13_F7.
_8E&_96_E1_C3J\$ _FA_BC_85_CC_F0_EC_EC_CC_ED_86_B5_84L_BE_1B_0C_E0_8D_90w2_E6s_CEb2WrE_CC_92_91+6_E34!R_F1_05_07_F2d.
_15_F94_CB_12_93_D9o_A96\$KcjX<&'_C7_C3_D3_C1p8_18_9E_DA_87_1F_19_1B_13d_AE_81_BB_A0Y_12-S_1A_07_3_E1,
[_E8px2_1A_9D_9E_1D_C3_DA_C1_C0_8A_B1d4_BE_B0['+f_A8_DD;`_FF_CD_F8_FA_BCw)_13_C3_123_98nS_D6#_91_BB:_EF_19_F6`BT_E4%
_89_96Tif_CE?Mo_06_A3_1E=%_C3_8D`_17_AFR_1A-_D9_89_97_1D_D4_9A_D3L_18rK_17_E3/_86l_A4_BA_D7_93_D0-v_1B_B5_D9
F_0C_F0_F3l"_AD{d_C5bN_CF{:R_8C%_D6z_CF_C8g_BBaE_15_D8hL_8E_D3_87_F2_DFK_FB_10_14_8Fy_B2h}
_FA_E7_11_FC7_93_F1_B6_EF_FC_E4su_C7sXY_FA
{yd_1F_CFht_BFP2K_E2A\$ _85Tc_F2_FD_D5_E8_EA_F5_F5_89_7F>_07_0B_E6t_C5_C5vL_FE_C9TL_13_DA'
_1A<e_A0_99_E2_F3_97_BBU_9A_FF_0EF_18_0ES_E3n_A2_B2_03*_F8_02_94_89_C0_CAL_15R_C6|_1D_AC(O_EER0\._A8t_CE7&_8A
j_F8_9A921_D7_A9_A0_C0_DD_D0_99^_AC_8F_CDrLf_C7_C7_85&_CEn_83_994F_AE_C6N_C5_D2}
_C1_E6fLhfd_E568_E4_B2r_7F_BF_85_9D_BD_A4_8A_99_1Ax_FE'9_13_7F;
7_E1_C9_F0_E4_E7_E7_A3_CA#_EB_06c_A2_A5_E0_F1~_DB_DF_D8_97_7F~_C0_80h_BB;_F4u_A6_BC
_97_CCisv_96_CB_E5_E5_1C_1E_1F_FF_D0_C1_F4_A7_9B_D3_9B_9F_F7_D2_D6)Dn_D57_87?_95_8C_F3_D3_CE:e?_18!_CB_E2_E6_C6_8B6_93"
_DE_CB_89_AF_165F_CFK[_D4Oa_DC_1A_01H_D4_BA_CA_9D_9C_DF_F9_00_D7_9EI\$ _18_85m_E8_0B_B9_D7_80_0F_E4_87_D9p_A6
/_08_9A_BD_07_E7xu_C9v_C7[_ED_15_B0y_82_B9|_DA_1D_F4_80l_F9_CDc_FBJF_EAc_E5_A5_B5_93:-lsZ;
_0E_BF_F3N_B3_08#_BC_E5_8C_Ffb_1B_D7_18_DE_E1_E2:_1E_A2_F9F_E8V_EE_BD_C3<e_AF>v^_DD_CD)U_AC_A6_E3_C8[f_D4
_E6#_FFdT_11_A5
5_C3_1A_D4x<_89_01_EEX_DC
B_B9
_87_C2_BE_A4_A3_A3_C9_D85z_84_9A_15%_0B_E4=p_FAno&_FA_FB_1F
_DEuX_C3:_83|o_05_0B+y_EF_D4_BB_D7i_97{_8D_AE_CF._9F_D4_FC_F7_B9_BD@VK~'?<*_F9UE_BESP+}_DE'
_D7_E5_D5_C9_F0_C5M_D7_F6_85b_DB_FD_FB_CFn_CE_9E_8FN_8B_FD_C1HH_AF_C9_E2_8E_B6_02_D1_0E_E4_BB_FC_0Bp_A1_DFu_EC9jX_F3_C4,
_92_8A:_9E_89LX_87_95_0Fr_1D_0B_9E_DC_F7_0F-Zs_D0_91_C5_07_D7_D1_08_F5_CF1_B9_01_87_A5Y_CAu_E1_89-GR_CD_A6_ABu_87NU_D7=KJ_9Av-
_AB(_DAV_0B^^_DD\9F_EE_C5_C6C_82~_8D_19r_96%_EaK_08\$ _E8_A4#_F5_A7_AB_ABC_8BV_B6_E0_0F_F3_8A_7F_82_E5_AF_AF_BBa#_A4S_AA_A1s)
J_CD_9E(V)Z_AE@_EA_B1Ql_80-X_9Dh_15_9D_F7B_0E_EA_EA0_B3=_C0@_C8_85_0C_D2d_D1#T@'_E1:_83_B7p_B7_97shPKdmy_B5o_E1n_1D!
_1D_BD_C7_8EZ_88_E4
-CP_13_BA8_E8_CB_9Aj7k_A4._E5K_1Bkp_DB_82E_15_B1_A7_AF^_BF_BD&_EFo_C8_E5_FB_A7_D7_BFN?
_96_84_B5_E2_B5_F1_D8_13X_9D_F6_99@_A7_A7_D8_FC_BC_F7=_9D_C9_0C_9E_BD_C2_B7IH/_BE=Gh_1A_93_05_D3_BD_8BK_F7_E1_EF_E1_AA#]
_EC_C5G|_FB{8_CE_B9_B0Z_CAd_CE_17_C4^_Edg_EC/W^_97_A3^_13_B6_08p_F4_15_EE_07_99_B4*: _EE_E4_F1y_CF_FBD_CD2_A4h_DA_BF
{_8C_F1_DA`_AE_CA-_B9_D7t_C95_81_7F8_07_89}D0n_98_88_E4_8A_11_DB_Fff_1A_D2_BF_91_90_14_B5_B1_AB_-*_E0@_1A_A4_E0_9C]
_C2\$mW_E6_98_00_BD8"-_9D_1Bl_A3_12_15_9C_F0_0B_93_1C0_F4V_C3l_EB_A0A_15L_00_E2_CD
(_8A_01_CB_91_AE_9D_96P_81_D5_81_15_11n_BB_11N_DF_CDt6K_1E-_EDJO_DC_D2 w_EF)
_14_87_0B_E4_00_E7_03_C9&n_11`N_B62#_11_00_A1_82c_04_BA_B0_1A_F9_F6_A1_16%+F_13_B4_1E5%_95_C9_9B_E9_F46W_DB+_0C_E2S_D3
n_89a2D_11_F0_A8Q_9AT_A1)_C56_BF_01c_BD_94_99_88!{(_96
_1A1_B7_DD{_12_CE._C8_13l#_1CM_B5_91_9F_18s_11_AE_A9_C2_B9_98_9D_85<_89_D9C_80_1F'!<|Jfl._15_B3_C3&_9Ed_C8_1E_0E_DB_1D%
C_C5UY_99_B2u&aZ_8E_82v_F7_F2_C6_A3_C0_81B_19_A5VT_A0G)_E7"_A83_9B9_FDi_12C_BF_90_FCh_C8}"7p_86_D6_A2_DE_D4`_9D_06i_1B3}
_BFF_C9_19@_C7_B6~_1C_B9e_A3_OC|61_B0_K_E8_9Ar_818C_E2_OCI)_1B_841!C_D1\$b_AD_DE_80_84_91!@_01_01;
i_AE_8D_EE_93_14_9Ac_ED_EC_08uK_C1_FDGMh_0C)<_RX\$4-_B8_BB_DA_1B_D9U_18i_87_90_02_E4_1B
_E2^_0E_153_1F_A1_EF_E10_D7_9Cm_BE_19_AE_B8_C8_03_EDs_10_C8_C1%
_AA_C8_81_81_C7_E7s_86_A7S_0Cd_1B_C4_B2_14_AC_C7_E8_AA_9DH_DF_FA_8EN_05_84#_9C_9C_04_05_EDp_8E_8B_19_00|_D9_F0_154@1_CEu_1B_A4.

_0B>_80_9EZ_DC4S_C2_CEzh_90_FF_CB\;_AF(_8CE_C5_86n_B5W_AE_F4_ADU_17_A9_A6qw_16_04_92yl_173_C0>_C8M_CC_AA(E1k0+E+Z_96^_90|y_F3&.
3h_87_C4Ey_E2_B1_05_B2_AF6_D2A0M_B6_80_C6-y_F5/2_E2eCi4|_01K_E50_0B_AD_89_FB_87_8E_A4_1Cbn_8BU_12_1FU"_CB?
_8B9_16_C7Rq`lk_81_96_OCPz_A5_E8fQ&_A8_AA_A7_99_84_A7)3_DA_17_B3_80_B2_88_96_7F_06*_F5_C9B@_C1#_BE_C0_B5_15]
`6_80_AD_80_85k_AE_0C_806YJ|_CB_A5_F0|1_9D2;y_81
_F4[_9D_13@_F5_D6U_85_C8_C9_96_AF_10_C1z_BB_C2_E9_91_E1_BCJ_EB_A2_D2tq|_C4_07W%M_BA_88<_1B_14_BCB_A0_98aA_80_C7_E2_B2?
_94t_BE_00_9F1_7F</p></div>
<div data-bbox="33 955 327 968" data-label="Page-Footer">Sysnet Scanning Management System May 16, 2024</div>
<div data-bbox="871 955 928 968" data-label="Page-Footer">Page 95</div>

q_175_D0" _B3_D9_12+_E7%_13X_1Er_B1_AE_E7_F6EOX_02G_DF_E9_AB~a_CC_F5_A1_95_ED_F9kd_C2_00x_A4P_87_97_1E_14_CB_11K:
_CD_FFh_D1_D1u_1E)z-l6y_A2_E0_01_FE_12_A0_E1w_E81_B6_81q_B5_1B_00.x_9A-
_0B_E7_D8_0B_D9J_ED_1B_86_18_99_F1_84_AA_AD_ED_80|_0B_EA_F31_B9_B2_BD_8F_05FH_07_D0_8Eu_91b
_86L_EC<_1E_BAI_8E_B1_02H_E1_81u_Q_EE_AB_AD_84_B1_18_13u[_95Yz_D9_8C_0B0
_A9_02_80/v_C5_B8_ED_B1_AA_82Ln_828/_AE_1C_D4_82AK%
FdG_BB_DF_9E_C4_96_E8_97`_08_8COK_1AKq_B0Q_95_AE_83p_A8_E37_1C_EA_88D_BA_19_8C_ED_B5_ADP_07_92o_AB9_0E_9Dr_F9_BA\s_F9_B6_ECK_Bf

_AA_BF_FBs_A2_85_FF_D0_E0#_11_CB_FD_B8_D7 T_03_0B_F6_00a_83_E6_04_92^_FB_F5E>_A1U_85_BD)
_84_DB_06_975_86_89_8F2c_D9DX_A8_F09_8F_D0t_BE_B9_D8_85_FB_ED_9B[_8BC_12;l_FD_B4_CDwK_A5_8E7'
_D4_05_08_E8_BE_B6h_CC_9B_F6_8A_9C_FBj1R.9Q_F9c_C9_97_8Ao^[_B5e_90_AB_EDW_AD_13_1B_CF@_F4_7F_EE_CD_A6*

HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:40:00 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT
ETag: "2aa6-5f040bdba30ce-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3138
Content-Type: text/html

_1F_8B_08_00_00_00_00_00_03

HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:40:04 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT
ETag: "2aa6-5f040bdba30ce-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3138
Content-Type: text/html

_1F_8B_08_00_00_00_00_00_03_BDZ_EBs_DB6_12_FF_EE_BF_02U_A7_D3\$'_91_96_93_BA_B2'(&_F1c_D2_99_A4_F1\$_CA_DD_F5_93_0F"!
c_88_E0_01_A0d5_ED_FF~_BB_00H_F1%_CA_C95_D5_C4_91H_02_FB_C2_EEo_1F_D2_D1_E4_BB_AB_F7_97_D3_DFn_AF_C9_D2_AC_04_B9_FD_F4_FA_ED
/_97_A47_08_C3_7F= _BF_0C_C3_AB_E9_15_F9_F7_9B_E9_BB_B7d_18_1C_93_A9_A2_89_E6_86_CB_84_8A0_BC_FE_B5GzKc_D2q_18n6_9B`_F3<_90j_11N?
_84_0FHk_88_9B_FD_C7_81)_ED_0Cb_13_F7.
_8E&_96_E1_C3J\$_FA_BC_85_CC_F0_EC_EC_CC_ED_86_B5_84L_BE_1B_0C_E0_8D_90w2_E6s_CEb2WrE_CC_92_91+6_E34!R_F1_05_07_F2d.
_15_F94_CB_12_93_D9o_A96\$KcjX<&'_C7_C3_D3_C1p8_18_9E_DA_87_1F_19_1B_13d_AE_81_BB_A0Y_12-S_1A_07_3_E1,
[_E8px2_1A_9D_9E_1D_C3_DA_C1_C0_8A_B1d4_BE_B0['+f_A8_DD;`_FF_CD_F8_FA_BCw)_13_C3_123_98nS_D6#_91_BB:_EF_19_F6`BT_E4%
_89_96Tif_CE?Mo_06_A3_1E =%_C3_8D`_17_AFR_1A-_D9_89_97_1D_D4_9A_D3L_18rK_17_E3/_86l_A4_BA_D7_93_D0-v_1B_B5_D9
F_0C_F0_F3l"_AD{d_C5bN_CF{:R_8C%_D6z_CF_C8g_BBaE_15_D8hL_8E_D3_87_F2_DFK_FB_10_14_8Fy_B2h}
_FA_E7_11_FC7_93_F1_B6_EF_FC_E4su_C7sXY_FA
{yd_1F_CFht_BFP2K_E2A\$_85Tc_F2_FD_D5_E8_EA_F5_F5_89_7F>_07_0B_E6t_C5_C5vL_FE_C9TL_13_DA'
_1A<e_A0_99_E2_F3_97_BBU_9A_FF_0EF_18_0ES_E3n_A2_B2_03*_F8_02_94_89_C0_CAL_15R_C6|_1D_AC(O_EER0\._A8t_CE7&_8A
j_F8_9A921_D7_A9_A0_C0_DD_D0_99^_AC_8F_CDrLF_C7_C7_85&_CEn_83_994F_AE_C6N_C5_D2}
_C1_E6fLhfd_E568_E4_B2r_7F_BF_85_9D_BD_A4_8A_99_1Ax_FE'9_13_7F;
7_E1_C9_F0_E4_E7_E7_A3_CA#_EB_06c_A2_A5_E0_F1~_DB_DF_D8_97_7F~_C0_80h_BB;_F4u_A6_BC
_97_CCisv_96_CB_E5_E5_1C_1E_1F_FF_D0_C1_F4_A7_9B_D3_9B_9F_F7_D2_D6)Dn_D57_87?_95_8C_F3_D3_CE:e?_18!_CB_E2_E6_C6_8B6_93"
_DE_CB_89_AF_165F_CFK[^_D4Oa_DC_1A_01H_D4_BA_CA_9D_9C_DF_F9_00_D7_9EI\$_18_85m_E8_0B_B9_D7_80_0F_E4_87_D9p_A6
/_08_9A_BD_07_E7xu_C9v_C7[_ED_15_B0y_82_B9l/_DA_1D_F4_80l_F9_CdC_FBjF_EAc_E5_A5_B5_93:-lsZ;
_0E_BF_F3N_B3_08#_BC_E5_8C_Ffb_1B_D7_18_DE_E1_E2:_1E_A2_F9F_E8V_EE_BD_C3<e_AF>v^_DD_CD)U_AC_A6_E3_C8[f_D4
_E6#_FFdT_11_A5
5_C3_1A_D4x<_89_01_EEX_DC

B_B9
_87_C2_BE_A4_A3_A3_C9_D85z_84_9A_15%_0B_E4=p_FAno&_FA_FB_1F
_DEuX_C3:_83|o_05_0B+y_EF_D4_BB_D7i_97{ _8D_AE_CF._9F_D4_FC_F7_B9_BD@VK~'?<*_F9UE_BESP+}_DE'
_D7_E5_D5_C9_F0_C5M_D7_F6_85b_DB_FD_FB_CFn_CE_9E_8FN_8B_FD_C1\HH_AF_C9_E2_8E_B6_02_D1_0E_E4_BB_FC_0Bp_A1_DFu_EC9jX_F3_C4,
_92_8A:_9E_89LX_87_95_0Fr_1D_0B_9E_DC_F7_0F-Zs_D0_91_C5_07_D7_D1_08_F5_CF1_B9_01_87_A5Y_CAu_E1_89-GR_CD_A6_ABu_87NU_D7=KJ_9Av-
_AB(_DAV_0B^^_DD_9F_EE_C5_C6C_82~_8D_19r_96%_EaK_08\$ _E8_A4#_F5_A7_AB_ABC_8BV_B6_E0_0F_F3_8A_7F_82_E5_AF_AF_BBa#_A4S_AA_A1s)
J_CD_9E{V}Z_AE@_EA_B1Ql_80-X_9Dh_15_9D_F7B_0E_EA_EA0_B3=_C0@_C8_85_0C_D2d_D1#T@'_E1:_83_B7p_B7_97shPKdmy_B5o_E1n_1D!
_1D_BD_C7_8EZ_88_E4
-CP_13_BA8_E8_CB_9Aj7k_A4_.E5K_1Bkp_DB_82E_15_B1_A7_AF^_BF_BD&_EFo_C8_E5_FB_A7_D7_BFN?
_96_84_B5_E2_B5_F1_D8_13X_9D_F6_99@_A7_A7_D8_FC_BC_F7=_9D_C9_0C_9E_BD_C2_B7IH/_BE=Gh_1A_93_05_D3_BD_8BK_F7_E1_EF_E1_AA#]
_EC_C5G|_FB{8_CE_B9_B0Z_CAd_CE_17_C4^_EDg_EC/W^_97_A3^_13_B6_08p_F4_15_EE_07_99_B4*: _EE_E4_F1y_CF_FBD_CD2_A4h_DA_BF
{_8C_F1_DA`_AE_CA-_B9_D7t_C95_81_7F8_07_89}_D0n_98_88_E4_8A_11_DB_FFi_1A_D2_BF_91_90_14_B5_B1_AB_*_E0@_1A_A4_E0_9C]
_C2\$mW_E6_98_00_BD8"-_9D_1Bl_A3_12_15_9C_F0_0B_93_1C0_F4V_C3l_EB_A0A_15L_00_E2_CD
(_8A_01_CB_91_AE_9D_96P_81_D5_81_15_11n_BB_11N_DF_CDt6K_1E-_EDJO_DC_D2 w_EF)
_14_87_0B_E4_00_E7_03_C9&n_11`N_B62#_11_00_A1_82c_04_BA_B0_1A_F9_F6_A1_16%+F_13_B4_1E5%_95_C9_9B_E9_F46W_DB+_0C_E2S_D3
n_89a2D_11_F0_A8Q_9AT_A1)_C56_BF_01c_BD_94_99_88l{(_96
_1A1_B7_DD{_12_CE._C8_13l#_1CM_B5_91_9F_18s_11_AE_A9_C2_B9_98_9D_85<_89_D9C_80_1F'!<|Jfl._15_B3_C3&_9Ed_C8_1E_0E_DB_1D%
C_C5UY_99_B2u&aZ_8E_82v_F7_F2_C6_A3_C0_81B_19_A5VT_A0G)_E7"_A83_9B9_FDi_12C_BF_90_FCh_C8}"7p_86_D6_A2_DE_D4`_9D_06i_1B3}
_BFF_C9_19@_C7_B6~_1C_B9e_A3_OC|61_B0_K_E8_9Ar_818C_E2_OCI)_1B_841!C_D1\$b_AD_DE_80_84_91!@_01_01;
i_AE_8D_EE_93_14_9Ac_ED_EC_08uK_C1_FDGMh_0C)<,RX\$4-_B8_BB_DA_1B_D9U_18i_87_90_02_E4_1B
_E2^_0E_153_1F_A1_EF_E10_D7_9Cm_BE_19_AE_B8_C8_03_EDs_10_C8_C1%
_AA_C8_81_81_C7_E7s_86_A7S_0Cd_1B_C4_B2_14_AC_C7_E8_AA_9DH_DF_FA_8EN_05_84#_9C_9C_04_05_EDp_8E_8B_19_00|_D9_F0_154@1_CEu_1B_A4

_0B>_80_9EZ_DC4S_C2_CEzh_90_FF_CB\;_AF(_8CE_C5_86n_B5W_AE_F4_ADU_17_A9_A6qw_16_04_92yl_173_C0>_C8M_CC_AA(E1k0+E+Z_96^_90)y_F3&
3h_87_C4Ey_E2_B1_05_B2_AF6_D2A0M_B6_80_C6-y_F5/2_E2eCi4]_01K_E50_0B_AD_89_FB_87_8E_A4_1Cbn_8BU_12_1FU"_CB?
_8B9_16_C7Rq`lk_81_96_OCPz_A5_E8fQ&_A8_AA_A7_99_84_A7)3_DA_17_B3_80_B2_88_96_7F_06*_F5_C9B@_C1#_BE_C0_B5_15]
`6_80_AD_80_85k_AE_0C_806YJ]_CB_A5_F0\1_9D2;y_81
_F4[_9D_13@_F5_D6U_85_C8_C9_96_AF_10_C1z_BB_C2_E9_91_E1_BCJ_EB_A2_D2tq]_C4_07W%M_BA_88<_1B_14_BCB_A0_98aA_80_C7_E2_B2?
_94t_BE_00_9F1_7F
q_175_D0"_B3_D9_12+_E7%_13X_1Er_B1_AE_E7_F6EOX_02G_DF_E9_AB~a_CC_F5_A1_95_ED_F9kd_C2_00x_A4P_87_97_1E_14_CB_11K:
_CD_Ffh_D1_D1u_1E)z-l6y_A2_E0_01_FE_12_A0_E1w_E81_B6_81q_B5_1B_00.x_9A-
_0B_E7_D8_0B_D9J_ED_1B_86_18_99_F1_84_AA_AD_ED_80|_0B_EA_F31_B9_B2_BD_8F_05FH_07_D0_8Eu_91b
_86L_EC<_1E_BAI_8E_B1_02H_E1_81u_Q_EE_AB_AD_84_B1_18_13u[_95Yz_D9_8C_0B0
_A9_02_80/v_C5_B8_ED_B1_AA_82Ln_828/_AE_1C_D4_82AK%
FdG_BB_DF_9E_C4_96_E8_97`_08_8COK_1AKq_B0Q_95_AE_83p_A8_E37_1C_EA_88D_BA_19_8C_ED_B5_ADP_07_92o_AB9_0E_9Dr_F9_BA\s_F9_B6_ECK_Bf

_AA_BF_FBs_A2_85_FF_D0_E0#_11_CB_FD_B8_D7 T_03_0B_F6_00a_83_E6_04_92^_FB_F5E>_A1U_85_BD)
_84_DB_06_975_86_89_8F2c_D9DX_A8_F09_8F_D0t_BE_B9_D8_85_FB_ED_9B[_8BC_12;l_FD_B4_CDwK_A5_8E7'
_D4_05_08_E8_BE_B6h_CC_9B_F6_8A_9C_FBj1R_9Q_F9c_C9_97_8Ao^(_B5e_90_AB_EDW_AD_13_1B_CF@_F4_7F_EE_CD_A6*


HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:40:09 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT
ETag: "2aa6-5f040bdba30ce-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3138
Content-Type: text/html

_1F_8B_08_00_00_00_00_00_03

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 3 

QID: 48001

Category: Information gathering

CVE ID: -

Vendor Reference: [Content-Security-Policy](#)

Bugtraq ID: -

Last Update: 2019-03-11 17:50:46.0

THREAT:
The HTTP Content-Security-Policy response header allows web site administrators to control resources the user agent is allowed to load for a given page. This helps guard against cross-site scripting attacks (XSS).

QID Detection Logic:
This QID detects the absence of the Content-Security-Policy HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A


RESULT:
Content-Security-Policy HTTP Header missing on port 443.
GET / HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

Web Server HTTP Protocol Versions port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 

QID: 45266

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2023-12-05 13:22:30.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

SMTP Banner

port 25 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2

QID: 74042

Category: Mail services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-11-02 08:52:43.0

THREAT:
The Simple Mail Transfer Protocol is a communication protocol for electronic mail transmission.

QID Detection Logic:
The QID checks for 220 status code in the banner of the response.

IMPACT:
NA

SOLUTION:
NA

RESULT:
220 basil.wingpath.co.uk ESMTP Postfix (Ubuntu)

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-04-29 12:49:04.0

THREAT:

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) **TCP/IP Fingerprint:** The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) **NetBIOS:** Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) **PHP Info:** PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) **SNMP:** The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB-II.system.sysDescr" for the operating system.

IMPACT:
Not applicable.

SOLUTION:
Not applicable.

RESULT:

Operating System Technique ID
Ubuntu/Linux TCP/IP Fingerprint U7254:
22

Host Uptime Based on TCP TimeStamp Option

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	82063
Category:	TCP/IP
CVE ID:	-

Vendor Reference: -
Bugtraq ID: -
Last Update: 2007-05-29 18:56:36.0

THREAT:
The TCP/IP stack on the host supports the TCP TimeStamp (kind 8) option. Typically the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. The result is given in the Result section below.
Some operating systems (e.g., MacOS, OpenBSD) use a non-zero, probably random, initial value for the timestamp. For these operating systems, the uptime obtained does not reflect the actual uptime of the host; the former is always larger than the latter.

IMPACT:
N/A

SOLUTION:
N/A


RESULT:
Based on TCP timestamps obtained via port 22, the host's uptime is 8 days, 10 hours, and 4 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

SMTP Service Detected port 25 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 2 
QID: 74145
Category: Mail services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2004-09-20 22:24:49.0

THREAT:
The Mail Service on this host can be identified from a remote system using SMTP fingerprinting. According to the results of this fingerprinting technique, the Mail Service name and version are listed below.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Name: Postfix, Version: Debian

Web Server HTTP Protocol Versions port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2023-12-05 13:22:30.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 80 port.GET / HTTP/1.1

Web Server HTTP Protocol Versions

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	45266
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2023-12-05 13:22:30.0

THREAT:
This QID lists supported HTTP protocol (HTTP 1.x or HTTP 2) from remote web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Remote Web Server supports HTTP version 1.x on 443 port.GET / HTTP/1.1

Web Applications and Plugins Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	2 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	45114
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-05-08 12:35:36.0

THREAT:

The result section of this QID lists web applications and plugins that were detected on the target using web application fingerprinting. This technique compares static files at known locations against precomputed hashes for versions of those files in all available releases. The technique is fast, low-bandwidth, non-invasive, generic, and highly automatable.

Following open source and free applications are currently supported:

Joomla!

MediaWiki

WordPress

phpBB

MovableType

Drupal

osCommerce

PHP-Nuke

Moodle

Liferay

Tikiwiki

Twiki

phpmyadmin

SPIP

Confluence(free versions)

Wikka

Wacko

Usemod

e107

Flyspray

AppRain

V-CMS

AjaxPloer/Pydio

eFront Learning Management System

vTigerCRM (Open source versions)

MyBB

- WebCalendar
- PivotX WebLog
- DokuWiki
- MODX Revolution
- MODX Evolution
- Collabtive
- Achievo
- Magento 1.x CE
- iCE Hrm (Opensource Version)
- AdaptCMS
- ownCloud
- HumHub
- Redaxscript
- phpwcms
- Wolf CMS
- Pligg CMS
- Zen Cart
- Xoops
- TYPO3
- Microweber

This QID is based on the [Blind Elephant project](#). For a complete list of supported web applications and plugins, please check the following link: [DOC-5480](#).

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

phpMyAdmin 4.9.4 in directory: /phpmyadmin/ Source: /themes/original/img/ajax_clock_small.gif

Scan Diagnostics

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page <http://wingpath.co.uk/> fetched. Status code:301, Content-Type:text/html, load time:55 milliseconds.

Ineffective Session Protection. no tests enabled.

Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)

[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase

CMSDetection: 1 vulnsigs tests, completed 38 requests, 1 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.

HSTS Analysis no tests enabled.

Maximum request count reached: 300

Collected 510 links overall in 0 hours 0 minutes duration.

Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)

BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 311) + files:(0 x 312) + directories:(9 x 27) + paths:(0 x 339) = total (243)

Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 339 inputs)

WS Directory Path manipulation: 9 vulnsigs tests, completed 243 requests, 4 seconds. Completed 243 requests of 243 estimated requests (100%). All tests completed.

WSEnumeration no tests enabled.

Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (70 tests, 19 inputs)

Batch #1 URI parameter manipulation (no auth): 70 vulnsigs tests, completed 1330 requests, 9 seconds. Completed 1330 requests of 1330 estimated requests (100%).

All tests completed.

Blind SQL manipulation - have 19 URI parameters,0 form fields - no tests enabled.

Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (16 tests, 19 inputs)

Batch #1 URI parameter time-based tests (no auth): 16 vulnsigs tests, completed 304 requests, 2 seconds. Completed 304 requests of 304 estimated requests (100%).

All tests completed.

Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (70 tests, 19 inputs)

Batch #2 URI parameter manipulation (no auth): 70 vulnsigs tests, completed 1330 requests, 12 seconds. Completed 1330 requests of 1330 estimated requests (100%).

All tests completed.

Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (16 tests, 19 inputs)

Batch #2 URI parameter time-based tests (no auth): 16 vulnsigs tests, completed 304 requests, 2 seconds. Completed 304 requests of 304 estimated requests (100%).

All tests completed.

Batch #3 URI parameter manipulation (no auth): estimated time < 1 minute (70 tests, 17 inputs)

Batch #3 URI parameter manipulation (no auth): 70 vulnsigs tests, completed 1257 requests, 9 seconds. Completed 1257 requests of 1190 estimated requests

(105.63%). All tests completed.

Blind SQL manipulation - have 17 URI parameters,0 form fields - no tests enabled.

Batch #3 URI parameter time-based tests (no auth): estimated time < 1 minute (16 tests, 17 inputs)

Batch #3 URI parameter time-based tests (no auth): 16 vulnsigs tests, completed 272 requests, 3 seconds. Completed 272 requests of 272 estimated requests (100%).

All tests completed.

Batch #4 WebCgiOob: estimated time < 10 minutes (135 tests, 1 inputs)

Batch #4 WebCgiOob: 135 vulnsigs tests, completed 3051 requests, 42 seconds. Completed 3051 requests of 53562 estimated requests (5.6962%). All tests completed.

XXE tests no tests enabled.

Arbitrary File Upload no tests enabled.

Arbitrary File Upload On Status OK no tests enabled.

HTTP call manipulation no tests enabled.

SSL Downgrade. no tests enabled.

Open Redirect no tests enabled.

CSRF no tests enabled.

Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 319 inputs)

Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 319 estimated requests (0%). All tests completed.

Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 1 inputs)

Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 5202 requests, 33 seconds. Completed 5202 requests of 5148 estimated requests (101.049%). XSS

optimization removed 8294 links. All tests completed.

Batch #4 Header manipulation: estimated time < 10 minutes (47 tests, 286 inputs)

Batch #4 Header manipulation: 47 vulnsigs tests, completed 18207 requests, 112 seconds. Completed 18207 requests of 37180 estimated requests (48.9699%). XSS optimization removed 8294 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 150 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 151 requests, 1 seconds. Completed 151 requests of 150 estimated requests (100.667%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

htpoxxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 311) + files:(0 x 312) + directories:(4 x 27) + paths:(11 x 339) = total (3837)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 339 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 3120 requests, 28 seconds. Completed 3120 requests of 3837 estimated requests (81.3135%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 311) + files:(4 x 312) + directories:(94 x 27) + paths:(5 x 339) = total (5481)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 339 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 4796 requests, 54 seconds. Completed 4796 requests of 5481 estimated requests (87.5023%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 1 hour (576 tests, 1 inputs)

Batch #5 WebCgiGeneric: 576 vulnsigs tests, completed 32030 requests, 402 seconds. Completed 32030 requests of 270861 estimated requests (11.8253%). All tests completed.

Duration of Crawl Time: 23.00 (seconds)

Duration of Test Phase: 713.00 (seconds)

Total Scan Time: 736.00 (seconds)

Total requests made: 72233

Average server response time: 0.06 seconds

Average browser load time: 0.06 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found

External Links Discovered

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1

QID: 150010

Category: Web Application

CVE ID: -

Vendor Reference: -
Bugtraq ID: -
Last Update: 2020-02-19 18:30:56.0

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Number of links: 43
<https://www.facebook.com/wingpath>
<https://www.americanexpress.com/>
<https://www.se.com/>
<https://twitter.com/WingpathUK>
<http://www.paessler.com/tools/mibimporter>
<http://www.paypal.com/>
<http://modbus.control.com/>
<http://www.modbus.org/>
<http://www.mastercard.com/>
<http://www.emersonprocess.com/>
<http://www.emersonprocess.com/daniel/default.htm>
[http://www05.abb.com/global/scot/scot267.nsf/veritydisplay/e2cc269455559c3d85256cd300640eff/\\$file/2100741AIAA.pdf](http://www05.abb.com/global/scot/scot267.nsf/veritydisplay/e2cc269455559c3d85256cd300640eff/$file/2100741AIAA.pdf)
<http://www.java.com/>
<http://www.snmp4j.org/>
http://www.snmp4j.org/LICENSE-2_0.txt
<http://modbus.org/>
http://modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf
http://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf
http://modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf
http://modbus.org/docs/Modbus_over_serial_line_V1_02.pdf
http://modbus.org/docs/PI_MBUS_300.pdf
<http://modbus.org/specs.php>
<http://www.visa.com/>
<http://www2.emersonprocess.com/siteadmincenter/PM%20Daniel%20Documents/3-9000-545.pdf>
<http://tools.ietf.org/html/rfc1157>
<http://tools.ietf.org/html/rfc2578>
<http://tools.ietf.org/html/rfc2579>
<http://tools.ietf.org/html/rfc2580>
<http://tools.ietf.org/html/rfc3410>
<http://tools.ietf.org/html/rfc3411>
<http://tools.ietf.org/html/rfc3412>
<http://tools.ietf.org/html/rfc3413>
<http://tools.ietf.org/html/rfc3414>
<http://tools.ietf.org/html/rfc3415>
<http://tools.ietf.org/html/rfc3416>
<http://tools.ietf.org/html/rfc3417>
<http://tools.ietf.org/html/rfc3418>
<http://tools.ietf.org/html/rfc3584>
<http://tools.ietf.org/html/rfc4181>
<http://www.schneider-electric.com/>

http://logging.apache.org/log4j/1.2/
http://www.ietf.org/
http://www.apache.org/licenses/LICENSE-2.0.html

Apache Default Installation/Welcome Page Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	48065
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-11-21 11:18:00.0

THREAT:
The Apache default installation or "Welcome" page is installed on this server. This usually indicates a newly installed server which has not yet been configured properly and which may not be known about.

Detection Logic(unauthenticated):
QID will check for the apache default Installation/Welcome Page on apache server.

IMPACT:
Apache is installed by default and the user may not be aware that the web server is running. These servers are rarely patched and rarely monitored, providing hackers with a convenient target that is not likely to trip any alarms.

SOLUTION:
Customers are recommended to disable default Apache welcome configuration.

RESULT:
HTTP/1.1 200 OK
Date: Thu, 16 May 2024 11:00:34 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT
ETag: "2aa6-5f040bdba30ce"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
Modified from the Debian original for Ubuntu
Last updated: 2016-11-16

See: <https://launchpad.net/bugs/1288690>

-->

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Ubuntu Default Page: It works</title>
<style type="text/css" media="screen">
```

```
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}
```

```
body, html {
padding: 3px 3px 3px 3px;
```

```
background-color: #D8DBE2;
```

```
font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}
```

```
div.main_page {
position: relative;
display: table;
```

```
width: 800px;
```

```
margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding: 0px 0px 0px 0px;
```

```
border-width: 2px;
border-color: #212738;
border-style: solid;
```

```
background-color: #FFFFFF;
```

```
text-align: center;
}
```

```
div.page_header {
height: 99px;
width: 100%;
```

```
background-color: #F5F6F7;
}
```

```
div.page_header span {
margin: 15px 0px 0px 50px;
```

```
font-size: 180%;
font-weight: bold;
}
```

```
div.page_header img {
```

margin: 3px 0px 0px 40px;

border: 0px 0px 0px;
}

div.table_of_contents {
clear: left;

min-width: 200px;

margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

div.table_of_contents_item {
clear: left;

width: 100%;

margin: 4px 0px 0px 0px;

background-color: #FFFFFF;

color: #000000;
text-align: left;
}

div.table_of_contents_item a {
margin: 6px 0px 0px 6px;
}

div.content_section {
margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

div.content_section_text {
padding: 4px 8px 4px 8px;

color: #000000;
font-size: 100%;
}

div.content_section_text pre {
margin: 8px 0px 8px 0px;
padding: 8px 8px 8px 8px;

border-width: 1px;
border-style: dotted;
border-color: #000000;

```
background-color: #F5F6F7;
```

```
font-style: italic;  
}
```

```
div.content_section_text p {  
margin-bottom: 6px;  
}
```

```
div.content_section_text ul, div.content_section_text li {  
padding: 4px 8px 4px 16px;  
}
```

```
div.section_header {  
padding: 3px 6px 3px 6px;
```

```
background-color: #8E9CB2;
```

```
color: #FFFFFF;  
font-weight: bold;  
font-size: 112%;  
text-align: center;  
}
```

```
div.section_header_red {  
background-color: #CD214F;  
}
```

```
div.section_header_grey {  
background-color: #9F9386;  
}
```

```
.floating_element {  
position: relative;  
float: left;  
}
```

```
div.table_of_contents_item a,  
div.content_section_text a {  
text-decoration: none;  
font-weight: bold;  
}
```

```
div.table_of_contents_item a:link,  
div.table_of_contents_item a:visited,  
div.table_of_contents_item a:active {  
color: #000000;  
}
```

```
div.table_of_contents_item a:hover {  
background-color: #000000;
```

```
color: #FFFFFF;  
}
```

```
div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
background-color: #DCDFE6;

color: #000000;
}

div.content_section_text a:hover {
background-color: #000000;

color: #DCDFE6;
}

div.validator {
}
</style>
</head>
<body>
<div class="main_page">
<div class="page_header floating_element">

<span class="floating_element">
Apache2 Ubuntu Default Page
</span>
</div>
<!-- <div class="table_of_contents floating_element">
<div class="section_header section_header_grey">
TABLE OF CONTENTS
</div>
<div class="table_of_contents_item floating_element">
<a href="#about">About</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#changes">Changes</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#scope">Scope</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#files">Config files</a>
</div>
</div>
-->
<div class="content_section floating_element">

<div class="section_header section_header_red">
<div id="about"></div>
It works!
</div>
<div class="content_section_text">
<p>
This is the default welcome page used to test the correct
operation of the Apache2 server after installation on Ubuntu systems.
It is based on the equivalent page on Debian, from which the Ubuntu Apache
```


packaging is derived.

If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance.

If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is fully documented in `/usr/share/doc/apache2/README.Debian.gz`. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the [manual](/manual) if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for

incoming connections, and this file can be customized anytime.

Configuration files in the <tt>mods-enabled/</tt>, <tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.

They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers

<tt>

a2enmod,

a2dismod,

</tt>

<tt>

a2ensite,

a2dissite,

</tt>

and

<tt>

a2enconf,

a2disconf

</tt>. See their respective man pages for detailed information.

The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>. Calling <tt>/usr/bin/apache2</tt> directly will not work with the default configuration.

</div>

<div class="section_header">

<div id="docroot"></div>

Document Roots

</div>

<div class="content_section_text">

<p>

By default, Ubuntu does not allow access through the web browser to any file apart of those located in <tt>/var/www/</tt>, public_html directories (when enabled) and <tt>/usr/share/</tt> (for web applications). If your site is using a web document root located elsewhere (such as in <tt>/srv/</tt>) you may need to whitelist your document root directory in <tt>/etc/apache2/apache2.conf</tt>.

</p>

<p>

The default Ubuntu document root is <tt>/var/www/html</tt>. You can make your own virtual hosts under /var/www. This is different to previous releases which provides better security out of the box.

</div>Reporting Problems</div><div class="content_section_text"><p>Please use the <tt>ubuntu-bug</tt> tool to report bugs in the Apache2 package with Ubuntu. However, check existing bug reports before reporting a new bug.</p><p>Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.</p></div>

</div></div><div class="validator"></div></body></html>

Apache Default Installation/Welcome Page Detected on port 443.

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-04-22 02:37:57.0

Sysnet Scanning Management System May 16, 2024

Page 115

THREAT:

A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control lists (ACLs).

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Some of the ports filtered by the firewall are: 20, 21, 23, 53, 111, 135, 445, 1, 7, 11.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-21,23-24,26-79,81-442,444-6128,6130-65535

ICMP Replies Received

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	82040
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2003-01-16 20:14:30.0

THREAT:

ICMP (Internet Control and Error Message Protocol) is a protocol encapsulated in IP packets. ICMP's principal purpose is to provide a protocol layer that informs gateways of the inter-connectivity and accessibility of other gateways or hosts.

We have sent the following types of packets to trigger the host to send us ICMP replies:

- Echo Request (to trigger Echo Reply)
- Timestamp Request (to trigger Timestamp Reply)
- Address Mask Request (to trigger Address Mask Reply)
- UDP Packet (to trigger Port Unreachable Reply)
- IP Packet with Protocol >= 250 (to trigger Protocol Unreachable Reply)

Listed in the "Result" section are the ICMP replies that we have received.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

ICMP Reply Type Triggered By Additional Information

- Echo (type=0 code=0) Echo Request Echo Reply
- Time Stamp (type=14 code=0) Time Stamp Request 10:09:24

GMT

Links Rejected By Crawl Scope or Exclusion List

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-02-07 16:48:28.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:
Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:
A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:
Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

IP based excluded links:

Referrer-Policy HTTP Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Last Update:	2023-01-18 13:30:16.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

RESULT:

Referrer-Policy HTTP Header missing on 443 port.

GET / HTTP/1.1

Host: wingpath.co.uk

Connection: Keep-Alive

SSL Certificate will expire within next six months

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38600
Category:	General remote services
CVE ID:	-

Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-01-29 20:24:19.0

THREAT:

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

IMPACT:

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

SOLUTION:

Contact the certificate authority that signed your certificate to arrange for a renewal.

RESULT:

Certificate #0 CN=wingpath.co.uk The certificate will expire within six months: Aug 7 16:08:38 2024 GMT

Certificate #0 CN=coppermist.co.uk The certificate will expire within six months: Aug 5 16:07:13 2024 GMT

SSH Banner
port 22 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38050
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-10-30 16:31:24.0

THREAT:

Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network.

QID Detection Logic:

The QID checks for SSH in the banner of the response.

IMPACT:

NA

SOLUTION:

NA

RESULT:

SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5

Links Crawled
port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

- NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
 - All the forms reported in QID 150152 (Forms Crawled)
 - All the forms in QID 150115 (Authentication Form Found)
 - Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 23.00
Number of links: 300
(This number excludes form requests and links re-requested during authentication.)

- https://wingpath.co.uk/
- https://wingpath.co.uk/contact.php
- https://wingpath.co.uk/custom_software.php
- https://wingpath.co.uk/docs/
- https://wingpath.co.uk/docs/modbus_tcp_specification.pdf
- https://wingpath.co.uk/docs/modmaster/address_mapping.html
- https://wingpath.co.uk/docs/modmaster/comdef_custom.html
- https://wingpath.co.uk/docs/modmaster/comdef_raw.html
- https://wingpath.co.uk/docs/modmaster/commands.html
- https://wingpath.co.uk/docs/modmaster/csvformat.html
- https://wingpath.co.uk/docs/modmaster/interface_settings.html
- https://wingpath.co.uk/docs/modmaster/logging.html
- https://wingpath.co.uk/docs/modmaster/message_tracing.html
- https://wingpath.co.uk/docs/modmaster/modmaster.html
- https://wingpath.co.uk/docs/modmaster/polling.html
- https://wingpath.co.uk/docs/modmaster/raw_tracing.html
- https://wingpath.co.uk/docs/modmaster/reg_tracing.html
- https://wingpath.co.uk/docs/modmaster/registers_adding.html
- https://wingpath.co.uk/docs/modmaster/releases.html
- https://wingpath.co.uk/docs/modmaster/tracing.html

<https://wingpath.co.uk/docs/modmaster/troubleshoot.html>
<https://wingpath.co.uk/docs/modmultisim/>
<https://wingpath.co.uk/docs/modmultisim/32-64bit.html>
https://wingpath.co.uk/docs/modmultisim/ModMultiSim_language.html
https://wingpath.co.uk/docs/modmultisim/ModMultiSim_variables.html
<https://wingpath.co.uk/docs/modmultisim/Values.html>
<https://wingpath.co.uk/docs/modmultisim/addreg.html>
https://wingpath.co.uk/docs/modmultisim/advanced_techniques.html
<https://wingpath.co.uk/docs/modmultisim/apf.html>
<https://wingpath.co.uk/docs/modmultisim/apptrace.html>
<https://wingpath.co.uk/docs/modmultisim/ar01s01.html>
<https://wingpath.co.uk/docs/modmultisim/chromat.html>
https://wingpath.co.uk/docs/modmultisim/csv_app.html
<https://wingpath.co.uk/docs/modmultisim/delallslaves.html>
<https://wingpath.co.uk/docs/modmultisim/delreg.html>
<https://wingpath.co.uk/docs/modmultisim/editaslave.html>
<https://wingpath.co.uk/docs/modmultisim/editenv.html>
<https://wingpath.co.uk/docs/modmultisim/editinterf.html>
<https://wingpath.co.uk/docs/modmultisim/editinterfleaf.html>
<https://wingpath.co.uk/docs/modmultisim/editlog.html>
<https://wingpath.co.uk/docs/modmultisim/editmisc.html>
<https://wingpath.co.uk/docs/modmultisim/editsets.html>
<https://wingpath.co.uk/docs/modmultisim/editslaves.html>
<https://wingpath.co.uk/docs/modmultisim/editslavesconnectedleaf.html>
<https://wingpath.co.uk/docs/modmultisim/envregs.html>
https://wingpath.co.uk/docs/modmultisim/example_settings.html
<https://wingpath.co.uk/docs/modmultisim/examples.html>
<https://wingpath.co.uk/docs/modmultisim/exportcsv.html>
https://wingpath.co.uk/docs/modmultisim/flow_computer.html
https://wingpath.co.uk/docs/modmultisim/gas_blender.html
<https://wingpath.co.uk/docs/modmultisim/general.html>
<https://wingpath.co.uk/docs/modmultisim/importcsv.html>
<https://wingpath.co.uk/docs/modmultisim/introduction.html>
https://wingpath.co.uk/docs/modmultisim/lexical_structure.html
https://wingpath.co.uk/docs/modmultisim/lift_pump_station.html
<https://wingpath.co.uk/docs/modmultisim/mainwindow.html>
<https://wingpath.co.uk/docs/modmultisim/mapaddr.html>
<https://wingpath.co.uk/docs/modmultisim/modmultisim.html>
<https://wingpath.co.uk/docs/modmultisim/opensets.html>
<https://wingpath.co.uk/docs/modmultisim/overlaidcoils.html>
https://wingpath.co.uk/docs/modmultisim/phrase_structure.html
https://wingpath.co.uk/docs/modmultisim/product_setup.html
<https://wingpath.co.uk/docs/modmultisim/progsimsintro.html>
<https://wingpath.co.uk/docs/modmultisim/quickstart.html>
https://wingpath.co.uk/docs/modmultisim/room_heater_on_off.html
https://wingpath.co.uk/docs/modmultisim/room_heater_pi.html
https://wingpath.co.uk/docs/modmultisim/room_heater_prop.html
<https://wingpath.co.uk/docs/modmultisim/runoptions.html>
<https://wingpath.co.uk/docs/modmultisim/runprogram.html>
<https://wingpath.co.uk/docs/modmultisim/runslaves.html>
<https://wingpath.co.uk/docs/modmultisim/savesets.html>
<https://wingpath.co.uk/docs/modmultisim/servem.html>
<https://wingpath.co.uk/docs/modmultisim/setsintro.html>
<https://wingpath.co.uk/docs/modmultisim/simulations.html>
<https://wingpath.co.uk/docs/modmultisim/slaveregs.html>
https://wingpath.co.uk/docs/modmultisim/syntax_summary.html

<https://wingpath.co.uk/docs/modmultisim/techniques.html>
<https://wingpath.co.uk/docs/modmultisim/tracing.html>
<https://wingpath.co.uk/docs/modmultisim/troubleshoot.html>
<https://wingpath.co.uk/docs/modmultisim/usingprog.html>
<https://wingpath.co.uk/docs/modmultisim/versionupdate.html>
<https://wingpath.co.uk/docs/modmultisim/winintro.html>
<https://wingpath.co.uk/docs/modsak/>
https://wingpath.co.uk/docs/modsak/address_mapping.html
https://wingpath.co.uk/docs/modsak/big_values.html
https://wingpath.co.uk/docs/modsak/comdef_custom.html
https://wingpath.co.uk/docs/modsak/comdef_raw.html
https://wingpath.co.uk/docs/modsak/command_define.html
<https://wingpath.co.uk/docs/modsak/commands.html>
<https://wingpath.co.uk/docs/modsak/csvformat.html>
https://wingpath.co.uk/docs/modsak/device_id_settings.html
https://wingpath.co.uk/docs/modsak/file_register_read_write.html
https://wingpath.co.uk/docs/modsak/file_register_table.html
https://wingpath.co.uk/docs/modsak/file_registers.html
https://wingpath.co.uk/docs/modsak/file_registers_adding.html
https://wingpath.co.uk/docs/modsak/general_settings.html
<https://wingpath.co.uk/docs/modsak/gui.html>
https://wingpath.co.uk/docs/modsak/interface_settings.html
<https://wingpath.co.uk/docs/modsak/introduction.html>
<https://wingpath.co.uk/docs/modsak/logging.html>
https://wingpath.co.uk/docs/modsak/message_tracing.html
<https://wingpath.co.uk/docs/modsak/modsak.html>
<https://wingpath.co.uk/docs/modsak/overview.html>
<https://wingpath.co.uk/docs/modsak/polling.html>
https://wingpath.co.uk/docs/modsak/polling_settings.html
https://wingpath.co.uk/docs/modsak/raw_tracing.html
https://wingpath.co.uk/docs/modsak/reg_tracing.html
https://wingpath.co.uk/docs/modsak/register_read_write.html
https://wingpath.co.uk/docs/modsak/register_table.html
<https://wingpath.co.uk/docs/modsak/registers.html>
https://wingpath.co.uk/docs/modsak/registers_adding.html
<https://wingpath.co.uk/docs/modsak/releases.html>
<https://wingpath.co.uk/docs/modsak/running.html>
https://wingpath.co.uk/docs/modsak/saving_configuration.html
https://wingpath.co.uk/docs/modsak/saving_file_registers.html
https://wingpath.co.uk/docs/modsak/saving_registers.html
https://wingpath.co.uk/docs/modsak/setting_up.html
<https://wingpath.co.uk/docs/modsak/settings.html>
<https://wingpath.co.uk/docs/modsak/tracing.html>
<https://wingpath.co.uk/docs/modsak/troubleshoot.html>
<https://wingpath.co.uk/docs/modslavesim/addreg.html>
<https://wingpath.co.uk/docs/modslavesim/apptrace.html>
https://wingpath.co.uk/docs/modslavesim/csv_app.html
<https://wingpath.co.uk/docs/modslavesim/editinterf.html>
<https://wingpath.co.uk/docs/modslavesim/mapaddr.html>
<https://wingpath.co.uk/docs/modslavesim/modslavesim.html>
<https://wingpath.co.uk/docs/modslavesim/simulations.html>
<https://wingpath.co.uk/docs/modslavesim/troubleshoot.html>
<https://wingpath.co.uk/docs/modslavesim/versionupdate.html>
<https://wingpath.co.uk/docs/modsnmp/>
<https://wingpath.co.uk/docs/modsnmp/acknowledgements.html>
https://wingpath.co.uk/docs/modsnmp/big_values.html

<https://wingpath.co.uk/docs/modsnmp/cache.html>
https://wingpath.co.uk/docs/modsnmp/command_line.html
<https://wingpath.co.uk/docs/modsnmp/constantoids.html>
https://wingpath.co.uk/docs/modsnmp/constoid_add.html
https://wingpath.co.uk/docs/modsnmp/constoid_edit.html
<https://wingpath.co.uk/docs/modsnmp/constoids.html>
https://wingpath.co.uk/docs/modsnmp/device_add.html
https://wingpath.co.uk/docs/modsnmp/device_delete.html
https://wingpath.co.uk/docs/modsnmp/device_edit.html
https://wingpath.co.uk/docs/modsnmp/device_reorder.html
https://wingpath.co.uk/docs/modsnmp/device_type_add.html
https://wingpath.co.uk/docs/modsnmp/device_type_delete.html
https://wingpath.co.uk/docs/modsnmp/device_type_edit.html
https://wingpath.co.uk/docs/modsnmp/device_type_save.html
https://wingpath.co.uk/docs/modsnmp/device_types.html
<https://wingpath.co.uk/docs/modsnmp/devices.html>
https://wingpath.co.uk/docs/modsnmp/engine_id.html
<https://wingpath.co.uk/docs/modsnmp/gui.html>
<https://wingpath.co.uk/docs/modsnmp/introduction.html>
<https://wingpath.co.uk/docs/modsnmp/logging.html>
<https://wingpath.co.uk/docs/modsnmp/mbserver.html>
<https://wingpath.co.uk/docs/modsnmp/mib.html>
https://wingpath.co.uk/docs/modsnmp/mib_settings.html
https://wingpath.co.uk/docs/modsnmp/modbus_interface_add.html
https://wingpath.co.uk/docs/modsnmp/modbus_interface_delete.html
https://wingpath.co.uk/docs/modsnmp/modbus_interface_edit.html
https://wingpath.co.uk/docs/modsnmp/modbus_interfaces.html
https://wingpath.co.uk/docs/modsnmp/modbus_settings.html
https://wingpath.co.uk/docs/modsnmp/modbus_variables.html
<https://wingpath.co.uk/docs/modsnmp/modbusdocs.html>
<https://wingpath.co.uk/docs/modsnmp/modsnmp.html>
https://wingpath.co.uk/docs/modsnmp/object_type_access.html
https://wingpath.co.uk/docs/modsnmp/object_type_add.html
https://wingpath.co.uk/docs/modsnmp/object_type_edit.html
https://wingpath.co.uk/docs/modsnmp/object_type_modbus.html
https://wingpath.co.uk/docs/modsnmp/object_type_snmp.html
https://wingpath.co.uk/docs/modsnmp/object_types.html
<https://wingpath.co.uk/docs/modsnmp/overview.html>
<https://wingpath.co.uk/docs/modsnmp/releases.html>
https://wingpath.co.uk/docs/modsnmp/response_handling.html
<https://wingpath.co.uk/docs/modsnmp/running.html>
https://wingpath.co.uk/docs/modsnmp/saving_settings.html
https://wingpath.co.uk/docs/modsnmp/serial_settings.html
<https://wingpath.co.uk/docs/modsnmp/server.html>
https://wingpath.co.uk/docs/modsnmp/server_settings.html
https://wingpath.co.uk/docs/modsnmp/server_unix.html
https://wingpath.co.uk/docs/modsnmp/server_windows.html
<https://wingpath.co.uk/docs/modsnmp/setup.html>
https://wingpath.co.uk/docs/modsnmp/snmp_interfaces.html
https://wingpath.co.uk/docs/modsnmp/snmp_oids.html
https://wingpath.co.uk/docs/modsnmp/snmp_user_add.html
https://wingpath.co.uk/docs/modsnmp/snmp_users.html
<https://wingpath.co.uk/docs/modsnmp/snmpdocs.html>
https://wingpath.co.uk/docs/modsnmp/socket_settings.html
<https://wingpath.co.uk/docs/modsnmp/tracing.html>
<https://wingpath.co.uk/docs/modsnmp/troubleshoot.html>

https://wingpath.co.uk/docs/modsnmp/user_delete.html
https://wingpath.co.uk/docs/modtest/comdef_custom.html
https://wingpath.co.uk/docs/modtest/comdef_raw.html
<https://wingpath.co.uk/docs/modtest/commands.html>
https://wingpath.co.uk/docs/modtest/interface_settings.html
<https://wingpath.co.uk/docs/modtest/logging.html>
https://wingpath.co.uk/docs/modtest/message_tracing.html
<https://wingpath.co.uk/docs/modtest/modtest.html>
https://wingpath.co.uk/docs/modtest/raw_tracing.html
<https://wingpath.co.uk/docs/modtest/releases.html>
<https://wingpath.co.uk/docs/modtest/tracing.html>
<https://wingpath.co.uk/docs/modtest/troubleshoot.html>
https://wingpath.co.uk/eval_register.php
<https://wingpath.co.uk/evaluate.php>
<https://wingpath.co.uk/evaluate.php?product=modmaster>
<https://wingpath.co.uk/evaluate.php?product=modmultisim>
<https://wingpath.co.uk/evaluate.php?product=modsak>
<https://wingpath.co.uk/evaluate.php?product=modslavesim>
<https://wingpath.co.uk/evaluate.php?product=modsnmp>
<https://wingpath.co.uk/evaluate.php?product=modtest>
https://wingpath.co.uk/exe/modmaster3.15_setup.exe
https://wingpath.co.uk/exe/modmultisim3.06_setup.exe
https://wingpath.co.uk/exe/modsak3.15_setup.exe
https://wingpath.co.uk/exe/modslavesim3.06_setup.exe
https://wingpath.co.uk/exe/modsnmp3.14_setup.exe
https://wingpath.co.uk/exe/modtest2.14_setup.exe
<https://wingpath.co.uk/favicon.ico>
https://wingpath.co.uk/full_register.php
<https://wingpath.co.uk/help.php>
<https://wingpath.co.uk/hptersms.php>
<https://wingpath.co.uk/image.php?file=modmultisim%2Fdeploy.svg%22desc%3DModMultiSim%2Bdeployment%2Bexample>
<https://wingpath.co.uk/image.php?file=modmultisim%2Feditreg.png%22desc%3DModMultiSim%2Bwindow%2Bfor%2Bediting%2Bsettings>
<https://wingpath.co.uk/image.php?file=modmultisim%2Fmain.png%22desc%3DModMultiSim%2Bmain%2Bwindow>
<https://wingpath.co.uk/image.php?file=modsak%2Fmain.png%22desc%3DModsak%2Bmain%2Bwindow>
<https://wingpath.co.uk/image.php?file=modslavesim%2Fdeploy.svg%22desc%3DModSlaveSim%2Bdeployment%2Bexample>
<https://wingpath.co.uk/image.php?file=modslavesim%2Fmain.png%22desc%3DModSlaveSim%2Bmain%2Bwindow>
<https://wingpath.co.uk/image.php?file=modsnmp%2Fdeploy.svg%22desc%3DModSnmp%2Bdeployment%2Bexample>
<https://wingpath.co.uk/image.php?file=modsnmp%2Fmain.png%22desc%3DModSnmp%2Bsscreenshot>
<https://wingpath.co.uk/jar/modmaster3.15.jar>
<https://wingpath.co.uk/jar/modmultisim3.06.jar>
<https://wingpath.co.uk/jar/modsak3.15.jar>
<https://wingpath.co.uk/jar/modslavesim3.06.jar>
<https://wingpath.co.uk/jar/modsnmp3.14.jar>
<https://wingpath.co.uk/jar/modtest2.14.jar>
<https://wingpath.co.uk/js/>
<https://wingpath.co.uk/licence.php>
<https://wingpath.co.uk/modbus/install.php>
<https://wingpath.co.uk/modbus/install.php?product=modmaster>
<https://wingpath.co.uk/modbus/install.php?product=modmultisim>
<https://wingpath.co.uk/modbus/install.php?product=modsak>
<https://wingpath.co.uk/modbus/install.php?product=modslavesim>
<https://wingpath.co.uk/modbus/install.php?product=modsnmp>
<https://wingpath.co.uk/modbus/install.php?product=modtest>
<https://wingpath.co.uk/modbus/modbus.php>
https://wingpath.co.uk/modbus/modbus_extensions.php
https://wingpath.co.uk/modbus/modbus_protocol.php

https://wingpath.co.uk/modbus/modbus_size_limits.php
<https://wingpath.co.uk/modbus/modmaster.php>
<https://wingpath.co.uk/modbus/modmultisim.php>
<https://wingpath.co.uk/modbus/modsak.php>
<https://wingpath.co.uk/modbus/modslavesim.php>
<https://wingpath.co.uk/modbus/modsnmp.php>
<https://wingpath.co.uk/modbus/modtest.php>
<https://wingpath.co.uk/modbus/resource.php?product=modmaster>
<https://wingpath.co.uk/modbus/resource.php?product=modmultisim>
<https://wingpath.co.uk/modbus/resource.php?product=modsak>
<https://wingpath.co.uk/modbus/resource.php?product=modslavesim>
<https://wingpath.co.uk/modbus/resource.php?product=modsnmp>
<https://wingpath.co.uk/modbus/resource.php?product=modtest>
<https://wingpath.co.uk/oldproducts.php>
<https://wingpath.co.uk/products.php>
<https://wingpath.co.uk/purchase.php>
<https://wingpath.co.uk/purchase.php?product0=12135>
<https://wingpath.co.uk/purchase.php?product0=123>
<https://wingpath.co.uk/purchase.php?product0=127>
<https://wingpath.co.uk/purchase.php?product0=128>
<https://wingpath.co.uk/purchase.php?product0=131>
<https://wingpath.co.uk/purchase.php?product0=135>
<https://wingpath.co.uk/purchase.php?product0=1635>
<https://wingpath.co.uk/purchase.php?product0=87>
<https://wingpath.co.uk/quote.php?product=12135>
<https://wingpath.co.uk/quote.php?product=123>
<https://wingpath.co.uk/quote.php?product=127>
<https://wingpath.co.uk/quote.php?product=128>
<https://wingpath.co.uk/quote.php?product=131>
<https://wingpath.co.uk/quote.php?product=135>
<https://wingpath.co.uk/quote.php?product=1635>
<https://wingpath.co.uk/quote.php?product=6135>
<https://wingpath.co.uk/register.php>
<https://wingpath.co.uk/resource/modmultisim/modmultisim.zip>
<https://wingpath.co.uk/resource/modsak/modsak.pdf>
<https://wingpath.co.uk/resource/modsak/modsak.zip>
<https://wingpath.co.uk/resource/modsnmp/Wingpath-MIB>
<https://wingpath.co.uk/resource/modsnmp/modsnmp.pdf>
<https://wingpath.co.uk/resource/modsnmp/modsnmp.service>
<https://wingpath.co.uk/resource/modsnmp/modsnmp.zip>
<https://wingpath.co.uk/resource/modsnmp/rc.modsnmp>
<https://wingpath.co.uk/transfer.php>
<https://wingpath.co.uk/update.php>
<https://wingpath.co.uk/update.php?product=modmaster>
<https://wingpath.co.uk/update.php?product=modmultisim>
<https://wingpath.co.uk/update.php?product=modsak>
<https://wingpath.co.uk/update.php?product=modslavesim>
<https://wingpath.co.uk/update.php?product=modsnmp>
<https://wingpath.co.uk/update.php?product=modtest>
<https://wingpath.co.uk/upgrade.php>
<https://wingpath.co.uk/upgrade.php?product=12135>
<https://wingpath.co.uk/upgrade.php?product=135>
<https://wingpath.co.uk/upgrade.php?product=1635>
<https://wingpath.co.uk/upgrade.php?product=3135>
<https://wingpath.co.uk/upgrade.php?product=6135>
<https://wingpath.co.uk/upgrade.php?product=modsnmp>

Default Web Page

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:
The Result section displays the default Web page for the Web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
GET / HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
GET / HTTP/1.1
Host: wingpath.co.uk
Connection: Keep-Alive
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
```

```
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://wingpath.co.uk/">here</a>.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at wingpath.co.uk Port 80</address>
</body></html>
```

Referrer-Policy HTTP Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	48131
Category:	Information gathering
CVE ID:	-
Vendor Reference:	Referrer-Policy
Bugtraq ID:	-
Last Update:	2023-01-18 13:30:16.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

RESULT:

Referrer-Policy HTTP Header missing on 443 port.
GET / HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

Degree of Randomness of TCP Initial Sequence Numbers

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	82045
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-11-19 21:53:59.0

THREAT:
TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Average change between subsequent TCP initial sequence numbers is 1272458765 with a standard deviation of 524081658. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5086 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

SSH daemon information retrievingport 22 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38047
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2018-04-04 16:20:22.0

THREAT:

SSH is a secure protocol, provided it is fully patched, properly configured, and uses FIPS approved algorithms.

For Red Hat ES 4:-	
SSH1 supported	yes
Supported authentication methods for SSH1	RSA,password
Supported ciphers for SSH1	3des,blowfish
SSH2 supported	yes
Supported keys exchange algorithm for SSH2	diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-
Supported decryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rij
Supported encryption ciphers for SSH2	aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,rij
Supported decryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac
Supported encryption mac for SSH2	hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac
Supported authentication methods for SSH2	publickey,gssapi-with-mic,password

IMPACT:

Successful exploitation allows an attacker to execute arbitrary commands on the SSH server or otherwise subvert an encrypted SSH channel with arbitrary data.

SOLUTION:

SSH version 2 is preferred over SSH version 1.

RESULT:

SSH1 supported no

SSH2 supported yes

Supported key exchange algorithms for SSH2 curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-sha256

Supported host key algorithms for SSH2 rsa-sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp256,ssh-ed25519

Supported decryption ciphers for SSH2 chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

Supported encryption ciphers for SSH2 chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com

Supported decryption macs for SSH2 umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

Supported encryption macs for SSH2 umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1

Supported decompression for SSH2 none,zlib@openssh.com

Supported compression for SSH2 none,zlib@openssh.com

Supported authentication methods for SSH2 publickey,password,keyboard-interactive

Links Crawled

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150009
Category:	Web Application

CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:

- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Duration of crawl phase (seconds): 25.00
Number of links: 300
(This number excludes form requests and links re-requested during authentication.)

- https://wingpath.co.uk/
- https://wingpath.co.uk/contact.php
- https://wingpath.co.uk/custom_software.php
- https://wingpath.co.uk/docs/
- https://wingpath.co.uk/docs/modbus_tcp_specification.pdf
- https://wingpath.co.uk/docs/modmaster/address_mapping.html
- https://wingpath.co.uk/docs/modmaster/comdef_custom.html
- https://wingpath.co.uk/docs/modmaster/comdef_raw.html
- https://wingpath.co.uk/docs/modmaster/commands.html
- https://wingpath.co.uk/docs/modmaster/csvformat.html
- https://wingpath.co.uk/docs/modmaster/interface_settings.html
- https://wingpath.co.uk/docs/modmaster/logging.html
- https://wingpath.co.uk/docs/modmaster/message_tracing.html
- https://wingpath.co.uk/docs/modmaster/modmaster.html
- https://wingpath.co.uk/docs/modmaster/polling.html
- https://wingpath.co.uk/docs/modmaster/raw_tracing.html
- https://wingpath.co.uk/docs/modmaster/reg_tracing.html
- https://wingpath.co.uk/docs/modmaster/registers_adding.html
- https://wingpath.co.uk/docs/modmaster/releases.html
- https://wingpath.co.uk/docs/modmaster/tracing.html
- https://wingpath.co.uk/docs/modmaster/troubleshoot.html
- https://wingpath.co.uk/docs/modmultisim/
- https://wingpath.co.uk/docs/modmultisim/32-64bit.html
- https://wingpath.co.uk/docs/modmultisim/ModMultiSim_language.html
- https://wingpath.co.uk/docs/modmultisim/ModMultiSim_variables.html
- https://wingpath.co.uk/docs/modmultisim/Values.html
- https://wingpath.co.uk/docs/modmultisim/addreg.html
- https://wingpath.co.uk/docs/modmultisim/advanced_techniques.html
- https://wingpath.co.uk/docs/modmultisim/apf.html
- https://wingpath.co.uk/docs/modmultisim/apptrace.html
- https://wingpath.co.uk/docs/modmultisim/ar01s01.html
- https://wingpath.co.uk/docs/modmultisim/chromat.html

https://wingpath.co.uk/docs/modmultisim/csv_app.html
<https://wingpath.co.uk/docs/modmultisim/delallslaves.html>
<https://wingpath.co.uk/docs/modmultisim/delreg.html>
<https://wingpath.co.uk/docs/modmultisim/editaslave.html>
<https://wingpath.co.uk/docs/modmultisim/editenv.html>
<https://wingpath.co.uk/docs/modmultisim/editinterf.html>
<https://wingpath.co.uk/docs/modmultisim/editinterfleaf.html>
<https://wingpath.co.uk/docs/modmultisim/editlog.html>
<https://wingpath.co.uk/docs/modmultisim/editmisc.html>
<https://wingpath.co.uk/docs/modmultisim/editsets.html>
<https://wingpath.co.uk/docs/modmultisim/editslaves.html>
<https://wingpath.co.uk/docs/modmultisim/editslavesconnectedleaf.html>
<https://wingpath.co.uk/docs/modmultisim/envregs.html>
https://wingpath.co.uk/docs/modmultisim/example_settings.html
<https://wingpath.co.uk/docs/modmultisim/examples.html>
<https://wingpath.co.uk/docs/modmultisim/exportcsv.html>
https://wingpath.co.uk/docs/modmultisim/flow_computer.html
https://wingpath.co.uk/docs/modmultisim/gas_blender.html
<https://wingpath.co.uk/docs/modmultisim/general.html>
<https://wingpath.co.uk/docs/modmultisim/importcsv.html>
<https://wingpath.co.uk/docs/modmultisim/introduction.html>
https://wingpath.co.uk/docs/modmultisim/lexical_structure.html
https://wingpath.co.uk/docs/modmultisim/lift_pump_station.html
<https://wingpath.co.uk/docs/modmultisim/mainwindow.html>
<https://wingpath.co.uk/docs/modmultisim/mapaddr.html>
<https://wingpath.co.uk/docs/modmultisim/modmultisim.html>
<https://wingpath.co.uk/docs/modmultisim/opensets.html>
<https://wingpath.co.uk/docs/modmultisim/overlaidcoils.html>
https://wingpath.co.uk/docs/modmultisim/phrase_structure.html
https://wingpath.co.uk/docs/modmultisim/product_setup.html
<https://wingpath.co.uk/docs/modmultisim/progsimsintro.html>
<https://wingpath.co.uk/docs/modmultisim/quickstart.html>
https://wingpath.co.uk/docs/modmultisim/room_heater_on_off.html
https://wingpath.co.uk/docs/modmultisim/room_heater_pi.html
https://wingpath.co.uk/docs/modmultisim/room_heater_prop.html
<https://wingpath.co.uk/docs/modmultisim/runoptions.html>
<https://wingpath.co.uk/docs/modmultisim/runprogram.html>
<https://wingpath.co.uk/docs/modmultisim/runslaves.html>
<https://wingpath.co.uk/docs/modmultisim/savesets.html>
<https://wingpath.co.uk/docs/modmultisim/servem.html>
<https://wingpath.co.uk/docs/modmultisim/setsintro.html>
<https://wingpath.co.uk/docs/modmultisim/simulations.html>
<https://wingpath.co.uk/docs/modmultisim/slavereg.html>
https://wingpath.co.uk/docs/modmultisim/syntax_summary.html
<https://wingpath.co.uk/docs/modmultisim/techniques.html>
<https://wingpath.co.uk/docs/modmultisim/tracing.html>
<https://wingpath.co.uk/docs/modmultisim/troubleshoot.html>
<https://wingpath.co.uk/docs/modmultisim/usingprog.html>
<https://wingpath.co.uk/docs/modmultisim/versionupdate.html>
<https://wingpath.co.uk/docs/modmultisim/winintro.html>
<https://wingpath.co.uk/docs/modsak/>
https://wingpath.co.uk/docs/modsak/address_mapping.html
https://wingpath.co.uk/docs/modsak/big_values.html
https://wingpath.co.uk/docs/modsak/comdef_custom.html
https://wingpath.co.uk/docs/modsak/comdef_raw.html
<https://wingpath.co.uk/docs/modsak/commands.html>

<https://wingpath.co.uk/docs/modsak/csvformat.html>
https://wingpath.co.uk/docs/modsak/device_id_settings.html
https://wingpath.co.uk/docs/modsak/file_register_read_write.html
https://wingpath.co.uk/docs/modsak/file_register_table.html
https://wingpath.co.uk/docs/modsak/file_registers.html
https://wingpath.co.uk/docs/modsak/file_registers_adding.html
https://wingpath.co.uk/docs/modsak/general_settings.html
<https://wingpath.co.uk/docs/modsak/gui.html>
https://wingpath.co.uk/docs/modsak/interface_settings.html
<https://wingpath.co.uk/docs/modsak/introduction.html>
<https://wingpath.co.uk/docs/modsak/logging.html>
https://wingpath.co.uk/docs/modsak/message_tracing.html
<https://wingpath.co.uk/docs/modsak/modsak.html>
<https://wingpath.co.uk/docs/modsak/overview.html>
<https://wingpath.co.uk/docs/modsak/polling.html>
https://wingpath.co.uk/docs/modsak/polling_settings.html
https://wingpath.co.uk/docs/modsak/raw_tracing.html
https://wingpath.co.uk/docs/modsak/reg_tracing.html
https://wingpath.co.uk/docs/modsak/register_read_write.html
https://wingpath.co.uk/docs/modsak/register_table.html
<https://wingpath.co.uk/docs/modsak/registers.html>
https://wingpath.co.uk/docs/modsak/registers_adding.html
<https://wingpath.co.uk/docs/modsak/releases.html>
<https://wingpath.co.uk/docs/modsak/running.html>
https://wingpath.co.uk/docs/modsak/saving_configuration.html
https://wingpath.co.uk/docs/modsak/saving_file_registers.html
https://wingpath.co.uk/docs/modsak/saving_registers.html
https://wingpath.co.uk/docs/modsak/setting_up.html
<https://wingpath.co.uk/docs/modsak/settings.html>
<https://wingpath.co.uk/docs/modsak/tracing.html>
<https://wingpath.co.uk/docs/modsak/troubleshoot.html>
<https://wingpath.co.uk/docs/modslavesim/addreg.html>
<https://wingpath.co.uk/docs/modslavesim/apprace.html>
https://wingpath.co.uk/docs/modslavesim/csv_app.html
<https://wingpath.co.uk/docs/modslavesim/editinterf.html>
<https://wingpath.co.uk/docs/modslavesim/mapaddr.html>
<https://wingpath.co.uk/docs/modslavesim/modslavesim.html>
<https://wingpath.co.uk/docs/modslavesim/simulations.html>
<https://wingpath.co.uk/docs/modslavesim/troubleshoot.html>
<https://wingpath.co.uk/docs/modslavesim/versionupdate.html>
<https://wingpath.co.uk/docs/modsnmp/>
<https://wingpath.co.uk/docs/modsnmp/acknowledgements.html>
https://wingpath.co.uk/docs/modsnmp/big_values.html
<https://wingpath.co.uk/docs/modsnmp/cache.html>
https://wingpath.co.uk/docs/modsnmp/command_line.html
<https://wingpath.co.uk/docs/modsnmp/constantoids.html>
https://wingpath.co.uk/docs/modsnmp/constoid_add.html
https://wingpath.co.uk/docs/modsnmp/constoid_edit.html
<https://wingpath.co.uk/docs/modsnmp/constoids.html>
https://wingpath.co.uk/docs/modsnmp/device_add.html
https://wingpath.co.uk/docs/modsnmp/device_delete.html
https://wingpath.co.uk/docs/modsnmp/device_edit.html
https://wingpath.co.uk/docs/modsnmp/device_reorder.html
https://wingpath.co.uk/docs/modsnmp/device_type_add.html
https://wingpath.co.uk/docs/modsnmp/device_type_delete.html
https://wingpath.co.uk/docs/modsnmp/device_type_edit.html

https://wingpath.co.uk/docs/modsnmp/device_type_save.html
https://wingpath.co.uk/docs/modsnmp/device_types.html
<https://wingpath.co.uk/docs/modsnmp/devices.html>
https://wingpath.co.uk/docs/modsnmp/engine_id.html
<https://wingpath.co.uk/docs/modsnmp/gui.html>
<https://wingpath.co.uk/docs/modsnmp/introduction.html>
<https://wingpath.co.uk/docs/modsnmp/logging.html>
<https://wingpath.co.uk/docs/modsnmp/mbserver.html>
<https://wingpath.co.uk/docs/modsnmp/mib.html>
https://wingpath.co.uk/docs/modsnmp/mib_settings.html
https://wingpath.co.uk/docs/modsnmp/modbus_interface_add.html
https://wingpath.co.uk/docs/modsnmp/modbus_interface_delete.html
https://wingpath.co.uk/docs/modsnmp/modbus_interface_edit.html
https://wingpath.co.uk/docs/modsnmp/modbus_interfaces.html
https://wingpath.co.uk/docs/modsnmp/modbus_settings.html
https://wingpath.co.uk/docs/modsnmp/modbus_variables.html
<https://wingpath.co.uk/docs/modsnmp/modbusdocs.html>
<https://wingpath.co.uk/docs/modsnmp/modsnmp.html>
https://wingpath.co.uk/docs/modsnmp/object_type_access.html
https://wingpath.co.uk/docs/modsnmp/object_type_add.html
https://wingpath.co.uk/docs/modsnmp/object_type_edit.html
https://wingpath.co.uk/docs/modsnmp/object_type_modbus.html
https://wingpath.co.uk/docs/modsnmp/object_type_snmp.html
https://wingpath.co.uk/docs/modsnmp/object_types.html
<https://wingpath.co.uk/docs/modsnmp/overview.html>
<https://wingpath.co.uk/docs/modsnmp/releases.html>
https://wingpath.co.uk/docs/modsnmp/response_handling.html
<https://wingpath.co.uk/docs/modsnmp/running.html>
https://wingpath.co.uk/docs/modsnmp/saving_settings.html
https://wingpath.co.uk/docs/modsnmp/serial_settings.html
<https://wingpath.co.uk/docs/modsnmp/server.html>
https://wingpath.co.uk/docs/modsnmp/server_settings.html
https://wingpath.co.uk/docs/modsnmp/server_unix.html
https://wingpath.co.uk/docs/modsnmp/server_windows.html
<https://wingpath.co.uk/docs/modsnmp/setup.html>
https://wingpath.co.uk/docs/modsnmp/snmp_interfaces.html
https://wingpath.co.uk/docs/modsnmp/snmp_oids.html
https://wingpath.co.uk/docs/modsnmp/snmp_user_add.html
https://wingpath.co.uk/docs/modsnmp/snmp_users.html
<https://wingpath.co.uk/docs/modsnmp/snmpdocs.html>
https://wingpath.co.uk/docs/modsnmp/socket_settings.html
<https://wingpath.co.uk/docs/modsnmp/tracing.html>
<https://wingpath.co.uk/docs/modsnmp/troubleshoot.html>
https://wingpath.co.uk/docs/modsnmp/user_delete.html
https://wingpath.co.uk/docs/modtest/comdef_custom.html
https://wingpath.co.uk/docs/modtest/comdef_raw.html
<https://wingpath.co.uk/docs/modtest/commands.html>
https://wingpath.co.uk/docs/modtest/interface_settings.html
<https://wingpath.co.uk/docs/modtest/logging.html>
https://wingpath.co.uk/docs/modtest/message_tracing.html
<https://wingpath.co.uk/docs/modtest/modtest.html>
https://wingpath.co.uk/docs/modtest/raw_tracing.html
<https://wingpath.co.uk/docs/modtest/releases.html>
<https://wingpath.co.uk/docs/modtest/tracing.html>
<https://wingpath.co.uk/docs/modtest/troubleshoot.html>
https://wingpath.co.uk/eval_register.php

<https://wingpath.co.uk/evaluate.php>
<https://wingpath.co.uk/evaluate.php?product=modmaster>
<https://wingpath.co.uk/evaluate.php?product=modmultisim>
<https://wingpath.co.uk/evaluate.php?product=modsak>
<https://wingpath.co.uk/evaluate.php?product=modslavesim>
<https://wingpath.co.uk/evaluate.php?product=modsnmp>
<https://wingpath.co.uk/evaluate.php?product=modtest>
https://wingpath.co.uk/exe/modmaster3.15_setup.exe
https://wingpath.co.uk/exe/modmultisim3.06_setup.exe
https://wingpath.co.uk/exe/modsak3.15_setup.exe
https://wingpath.co.uk/exe/modslavesim3.06_setup.exe
https://wingpath.co.uk/exe/modsnmp3.14_setup.exe
https://wingpath.co.uk/exe/modtest2.14_setup.exe
<https://wingpath.co.uk/favicon.ico>
https://wingpath.co.uk/full_register.php
<https://wingpath.co.uk/help.php>
<https://wingpath.co.uk/hptersms.php>
<https://wingpath.co.uk/image.php?file=modmultisim%2Fdeploy.svg%22desc%3DModMultiSim%2Bdeployment%2Bexample>
<https://wingpath.co.uk/image.php?file=modmultisim%2Feditreg.png%22desc%3DModMultiSim%2Bwindow%2Bfor%2Bediting%2Bsettings>
<https://wingpath.co.uk/image.php?file=modmultisim%2Fmain.png%22desc%3DModMultiSim%2Bmain%2Bwindow>
<https://wingpath.co.uk/image.php?file=modsak%2Fmain.png%22desc%3DModsak%2Bmain%2Bwindow>
<https://wingpath.co.uk/image.php?file=modslavesim%2Fdeploy.svg%22desc%3DModSlaveSim%2Bdeployment%2Bexample>
<https://wingpath.co.uk/image.php?file=modslavesim%2Fmain.png%22desc%3DModSlaveSim%2Bmain%2Bwindow>
<https://wingpath.co.uk/image.php?file=modsnmp%2Fdeploy.svg%22desc%3DModSnmp%2Bdeployment%2Bexample>
<https://wingpath.co.uk/image.php?file=modsnmp%2Fmain.png%22desc%3DModSnmp%2Bsscreenshot>
<https://wingpath.co.uk/jar/modmaster3.15.jar>
<https://wingpath.co.uk/jar/modmultisim3.06.jar>
<https://wingpath.co.uk/jar/modsak3.15.jar>
<https://wingpath.co.uk/jar/modslavesim3.06.jar>
<https://wingpath.co.uk/jar/modsnmp3.14.jar>
<https://wingpath.co.uk/jar/modtest2.14.jar>
<https://wingpath.co.uk/js/>
<https://wingpath.co.uk/licence.php>
<https://wingpath.co.uk/modbus/install.php>
<https://wingpath.co.uk/modbus/install.php?product=modmaster>
<https://wingpath.co.uk/modbus/install.php?product=modmultisim>
<https://wingpath.co.uk/modbus/install.php?product=modsak>
<https://wingpath.co.uk/modbus/install.php?product=modslavesim>
<https://wingpath.co.uk/modbus/install.php?product=modsnmp>
<https://wingpath.co.uk/modbus/install.php?product=modtest>
<https://wingpath.co.uk/modbus/modbus.php>
https://wingpath.co.uk/modbus/modbus_extensions.php
https://wingpath.co.uk/modbus/modbus_protocol.php
https://wingpath.co.uk/modbus/modbus_size_limits.php
<https://wingpath.co.uk/modbus/modmaster.php>
<https://wingpath.co.uk/modbus/modmultisim.php>
<https://wingpath.co.uk/modbus/modsak.php>
<https://wingpath.co.uk/modbus/modslavesim.php>
<https://wingpath.co.uk/modbus/modsnmp.php>
<https://wingpath.co.uk/modbus/modtest.php>
<https://wingpath.co.uk/modbus/resource.php?product=modmaster>
<https://wingpath.co.uk/modbus/resource.php?product=modmultisim>
<https://wingpath.co.uk/modbus/resource.php?product=modsak>
<https://wingpath.co.uk/modbus/resource.php?product=modslavesim>
<https://wingpath.co.uk/modbus/resource.php?product=modsnmp>
<https://wingpath.co.uk/modbus/resource.php?product=modtest>

https://wingpath.co.uk/oldproducts.php
https://wingpath.co.uk/products.php
https://wingpath.co.uk/purchase.php
https://wingpath.co.uk/purchase.php?product0=12135
https://wingpath.co.uk/purchase.php?product0=127
https://wingpath.co.uk/purchase.php?product0=128
https://wingpath.co.uk/purchase.php?product0=131
https://wingpath.co.uk/purchase.php?product0=1635
https://wingpath.co.uk/purchase.php?product0=3135
https://wingpath.co.uk/purchase.php?product0=6135
https://wingpath.co.uk/purchase.php?product0=87
https://wingpath.co.uk/quote.php?product=12135
https://wingpath.co.uk/quote.php?product=123
https://wingpath.co.uk/quote.php?product=128
https://wingpath.co.uk/quote.php?product=135
https://wingpath.co.uk/quote.php?product=1635
https://wingpath.co.uk/quote.php?product=3135
https://wingpath.co.uk/quote.php?product=6135
https://wingpath.co.uk/quote.php?product=87
https://wingpath.co.uk/register.php
https://wingpath.co.uk/resource/modmultisim/modmultisim.zip
https://wingpath.co.uk/resource/modsak/modsak.pdf
https://wingpath.co.uk/resource/modsak/modsak.zip
https://wingpath.co.uk/resource/modsnmp/Wingpath-MIB
https://wingpath.co.uk/resource/modsnmp/modsnmp.pdf
https://wingpath.co.uk/resource/modsnmp/modsnmp.service
https://wingpath.co.uk/resource/modsnmp/modsnmp.zip
https://wingpath.co.uk/resource/modsnmp/rc.modsnmp
https://wingpath.co.uk/transfer.php
https://wingpath.co.uk/update.php
https://wingpath.co.uk/update.php?product=37
https://wingpath.co.uk/update.php?product=81
https://wingpath.co.uk/update.php?product=modmaster
https://wingpath.co.uk/update.php?product=modmultisim
https://wingpath.co.uk/update.php?product=modsak
https://wingpath.co.uk/update.php?product=modslavesim
https://wingpath.co.uk/update.php?product=modsnmp
https://wingpath.co.uk/update.php?product=modtest
https://wingpath.co.uk/upgrade.php
https://wingpath.co.uk/upgrade.php?product=12135
https://wingpath.co.uk/upgrade.php?product=135
https://wingpath.co.uk/upgrade.php?product=1635
https://wingpath.co.uk/upgrade.php?product=3135
https://wingpath.co.uk/upgrade.php?product=6135


External Links Discovered

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150010

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-02-19 18:30:56.0

THREAT:
External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Number of links: 2
<https://bugs.launchpad.net/ubuntu/+source/apache2>
http://httpd.apache.org/docs/2.4/mod/mod_userdir.html


List of Web Directories

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 86672

Category: Web server

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2004-09-10 23:40:57.0

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Directory Source
/"><script>alert(document.domain)</ web
page

/admin/ web page
/help/ web page
/install/ web page
/secure/ web page
/manager/ web page
/crx/ web page
/crx/explorer/ web page
/crx/explorer/browser/ web page
/setup/ web page
/mics/ web page
/mics/scripts/ web page
/mics/scripts/mics/ web page
/Scripts/ web page
/Scripts/ReportServer/ web page

Scan Diagnostics

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

- THREAT:**
This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.
- IMPACT:**
The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.
- SOLUTION:**
No action is required.

RESULT:
Target web application page http://basil.wingpath.co.uk/ fetched. Status code:404, Content-Type:text/html, load time:57 milliseconds.
Ineffective Session Protection. no tests enabled.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 38 requests, 1 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.
HSTS Analysis no tests enabled.
Collected 1 links overall in 0 hours 0 minutes duration.

Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)

BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(9 x 1) + paths:(0 x 1) = total (9)

Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 1 inputs)

WS Directory Path manipulation: 9 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 9 estimated requests (100%). All tests completed.

WSEnumeration no tests enabled.

Batch #4 WebCgiOob: estimated time < 1 minute (135 tests, 1 inputs)

Batch #4 WebCgiOob: 135 vulnsigs tests, completed 9 requests, 0 seconds. Completed 9 requests of 158 estimated requests (5.6962%). All tests completed.

XXE tests no tests enabled.

Arbitrary File Upload no tests enabled.

Arbitrary File Upload On Status OK no tests enabled.

HTTP call manipulation no tests enabled.

SSL Downgrade. no tests enabled.

Open Redirect no tests enabled.

CSRF no tests enabled.

Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 1 inputs)

Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.

Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 0 inputs)

Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 1 inputs)

Batch #4 Header manipulation: 47 vulnsigs tests, completed 63 requests, 0 seconds. Completed 63 requests of 130 estimated requests (48.4615%). XSS optimization removed 29 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 1 requests, 0 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

httpoxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(4 x 1) + paths:(11 x 1) = total (15)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 1 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 14 requests, 0 seconds. Completed 14 requests of 15 estimated requests (93.3333%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(4 x 0) + directories:(94 x 1) + paths:(5 x 1) = total (99)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 1 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 98 requests, 1 seconds. Completed 98 requests of 99 estimated requests (98.9899%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 1 minute (576 tests, 1 inputs)

Batch #5 WebCgiGeneric: 576 vulnsigs tests, completed 189 requests, 1 seconds. Completed 189 requests of 799 estimated requests (23.6546%). All tests completed.

Duration of Crawl Time: 3.00 (seconds)

Duration of Test Phase: 2.00 (seconds)

Total Scan Time: 5.00 (seconds)

Total requests made: 425

Average server response time: 0.03 seconds

Average browser load time: 0.03 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found

TLS Secure Renegotiation Extension Support Information
 port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div></div>
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:
 Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
 N/A

SOLUTION:
 N/A

RESULT:
 TLS Secure Renegotiation Extension Status: supported.

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods
 port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div></div>
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2023-02-01 23:14:33.0

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH

TLSv1
CAMELLIA256-SHA RSA 2048 no 110 low
CAMELLIA128-SHA RSA 2048 no 110 low
AES256-SHA RSA 2048 no 110 low
AES128-SHA RSA 2048 no 110 low
SEED-SHA RSA 2048 no 110 low
DHE-RSA-CAMELLIA256-SHA DHE 2048 yes 110 low
DHE-RSA-CAMELLIA128-SHA DHE 2048 yes 110 low
DHE-RSA-AES256-SHA DHE 2048 yes 110 low
DHE-RSA-AES128-SHA DHE 2048 yes 110 low
DHE-RSA-SEED-SHA DHE 2048 yes 110 low
ADH-CAMELLIA256-SHA DHA 2048 yes 110 low
ADH-CAMELLIA128-SHA DHA 2048 yes 110 low
ADH-AES256-SHA DHA 2048 yes 110 low
ADH-AES128-SHA DHA 2048 yes 110 low
ADH-SEED-SHA DHA 2048 yes 110 low
ECDHE-RSA-AES256-SHA ECDHE x448 448 yes 224 low
ECDHE-RSA-AES256-SHA ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES256-SHA ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-AES256-SHA ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES256-SHA ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-AES128-SHA ECDHE x448 448 yes 224 low
ECDHE-RSA-AES128-SHA ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES128-SHA ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-AES128-SHA ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES128-SHA ECDHE secp521r1 521 yes 260 low
AECDH-AES256-SHA ECDHA x448 448 yes 224 low
AECDH-AES256-SHA ECDHA x25519 256 yes 128 low
AECDH-AES256-SHA ECDHA secp384r1 384 yes 192 low
AECDH-AES256-SHA ECDHA secp256r1 256 yes 128 low
AECDH-AES256-SHA ECDHA secp521r1 521 yes 260 low
AECDH-AES128-SHA ECDHA x448 448 yes 224 low
AECDH-AES128-SHA ECDHA x25519 256 yes 128 low
AECDH-AES128-SHA ECDHA secp384r1 384 yes 192 low
AECDH-AES128-SHA ECDHA secp256r1 256 yes 128 low
AECDH-AES128-SHA ECDHA secp521r1 521 yes 260 low
TLSv1.1
CAMELLIA256-SHA RSA 2048 no 110 low
CAMELLIA128-SHA RSA 2048 no 110 low
AES256-SHA RSA 2048 no 110 low
AES128-SHA RSA 2048 no 110 low
SEED-SHA RSA 2048 no 110 low
DHE-RSA-CAMELLIA256-SHA DHE 2048 yes 110 low
DHE-RSA-CAMELLIA128-SHA DHE 2048 yes 110 low
DHE-RSA-AES256-SHA DHE 2048 yes 110 low

DHE-RSA-AES128-SHA DHE 2048 yes 110 low
DHE-RSA-SEED-SHA DHE 2048 yes 110 low
ADH-CAMELLIA256-SHA DHA 2048 yes 110 low
ADH-CAMELLIA128-SHA DHA 2048 yes 110 low
ADH-AES256-SHA DHA 2048 yes 110 low
ADH-AES128-SHA DHA 2048 yes 110 low
ADH-SEED-SHA DHA 2048 yes 110 low
ECDHE-RSA-AES256-SHA ECDHE x448 448 yes 224 low
ECDHE-RSA-AES256-SHA ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES256-SHA ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-AES256-SHA ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES256-SHA ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-AES128-SHA ECDHE x448 448 yes 224 low
ECDHE-RSA-AES128-SHA ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES128-SHA ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-AES128-SHA ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES128-SHA ECDHE secp521r1 521 yes 260 low
AECDH-AES256-SHA ECDHA x448 448 yes 224 low
AECDH-AES256-SHA ECDHA x25519 256 yes 128 low
AECDH-AES256-SHA ECDHA secp384r1 384 yes 192 low
AECDH-AES256-SHA ECDHA secp256r1 256 yes 128 low
AECDH-AES256-SHA ECDHA secp521r1 521 yes 260 low
AECDH-AES128-SHA ECDHA x448 448 yes 224 low
AECDH-AES128-SHA ECDHA x25519 256 yes 128 low
AECDH-AES128-SHA ECDHA secp384r1 384 yes 192 low
AECDH-AES128-SHA ECDHA secp256r1 256 yes 128 low
AECDH-AES128-SHA ECDHA secp521r1 521 yes 260 low
TLSv1.2
AES256-SHA256 RSA 2048 no 110 low
AES128-SHA256 RSA 2048 no 110 low
AES256-CCM-8 RSA 2048 no 110 low
AES128-CCM-8 RSA 2048 no 110 low
AES256-CCM RSA 2048 no 110 low
AES128-CCM RSA 2048 no 110 low
ARIA256-GCM-SHA384 RSA 2048 no 110 low
ARIA128-GCM-SHA256 RSA 2048 no 110 low
CAMELLIA256-SHA256 RSA 2048 no 110 low
AES256-GCM-SHA384 RSA 2048 no 110 low
AES128-GCM-SHA256 RSA 2048 no 110 low
CAMELLIA256-SHA RSA 2048 no 110 low
CAMELLIA128-SHA RSA 2048 no 110 low
AES256-SHA RSA 2048 no 110 low
AES128-SHA RSA 2048 no 110 low
SEED-SHA RSA 2048 no 110 low
CAMELLIA128-SHA256 RSA 2048 no 110 low
DHE-RSA-AES256-GCM-SHA384 DHE 2048 yes 110 low
DHE-RSA-CHACHA20-POLY1305 DHE 2048 yes 110 low
DHE-RSA-ARIA256-GCM-SHA384 DHE 2048 yes 110 low
DHE-RSA-AES128-GCM-SHA256 DHE 2048 yes 110 low
DHE-RSA-ARIA128-GCM-SHA256 DHE 2048 yes 110 low
DHE-RSA-AES256-CCM DHE 2048 yes 110 low
DHE-RSA-AES128-CCM DHE 2048 yes 110 low
DHE-RSA-AES256-CCM-8 DHE 2048 yes 110 low
DHE-RSA-AES128-CCM-8 DHE 2048 yes 110 low
DHE-RSA-AES256-SHA256 DHE 2048 yes 110 low
DHE-RSA-CAMELLIA256-SHA256 DHE 2048 yes 110 low

DHE-RSA-CAMELLIA256-SHA DHE 2048 yes 110 low
DHE-RSA-AES128-SHA256 DHE 2048 yes 110 low
DHE-RSA-CAMELLIA128-SHA256 DHE 2048 yes 110 low
DHE-RSA-CAMELLIA128-SHA DHE 2048 yes 110 low
DHE-RSA-AES256-SHA DHE 2048 yes 110 low
DHE-RSA-AES128-SHA DHE 2048 yes 110 low
DHE-RSA-SEED-SHA DHE 2048 yes 110 low
ADH-CAMELLIA256-SHA256 DHA 2048 yes 110 low
ADH-CAMELLIA128-SHA256 DHA 2048 yes 110 low
ADH-AES256-GCM-SHA384 DHA 2048 yes 110 low
ADH-AES128-GCM-SHA256 DHA 2048 yes 110 low
ADH-CAMELLIA256-SHA DHA 2048 yes 110 low
ADH-AES256-SHA256 DHA 2048 yes 110 low
ADH-AES128-SHA256 DHA 2048 yes 110 low
ADH-CAMELLIA128-SHA DHA 2048 yes 110 low
ADH-AES256-SHA DHA 2048 yes 110 low
ADH-AES128-SHA DHA 2048 yes 110 low
ADH-SEED-SHA DHA 2048 yes 110 low
ECDHE-RSA-AES256-GCM-SHA384 ECDHE x448 448 yes 224 low
ECDHE-RSA-AES256-GCM-SHA384 ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-CHACHA20-POLY1305 ECDHE x448 448 yes 224 low
ECDHE-RSA-CHACHA20-POLY1305 ECDHE x25519 256 yes 128 low
ECDHE-RSA-CHACHA20-POLY1305 ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-CHACHA20-POLY1305 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-CHACHA20-POLY1305 ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-AES128-GCM-SHA256 ECDHE x448 448 yes 224 low
ECDHE-RSA-AES128-GCM-SHA256 ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-ARIA256-GCM-SHA384 ECDHE x448 448 yes 224 low
ECDHE-RSA-ARIA256-GCM-SHA384 ECDHE x25519 256 yes 128 low
ECDHE-RSA-ARIA256-GCM-SHA384 ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-ARIA256-GCM-SHA384 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-ARIA256-GCM-SHA384 ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-ARIA128-GCM-SHA256 ECDHE x448 448 yes 224 low
ECDHE-RSA-ARIA128-GCM-SHA256 ECDHE x25519 256 yes 128 low
ECDHE-RSA-ARIA128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-ARIA128-GCM-SHA256 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-ARIA128-GCM-SHA256 ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-AES256-SHA384 ECDHE x448 448 yes 224 low
ECDHE-RSA-AES256-SHA384 ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES256-SHA384 ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-AES256-SHA384 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES256-SHA384 ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-CAMELLIA256-SHA384 ECDHE x448 448 yes 224 low
ECDHE-RSA-CAMELLIA256-SHA384 ECDHE x25519 256 yes 128 low
ECDHE-RSA-CAMELLIA256-SHA384 ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-CAMELLIA256-SHA384 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-CAMELLIA256-SHA384 ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-AES128-SHA256 ECDHE x448 448 yes 224 low
ECDHE-RSA-AES128-SHA256 ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES128-SHA256 ECDHE secp384r1 384 yes 192 low

ECDHE-RSA-AES128-SHA256 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES128-SHA256 ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-CAMELLIA128-SHA256 ECDHE x448 448 yes 224 low
ECDHE-RSA-CAMELLIA128-SHA256 ECDHE x25519 256 yes 128 low
ECDHE-RSA-CAMELLIA128-SHA256 ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-CAMELLIA128-SHA256 ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-CAMELLIA128-SHA256 ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-AES256-SHA ECDHE x448 448 yes 224 low
ECDHE-RSA-AES256-SHA ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES256-SHA ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-AES256-SHA ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES256-SHA ECDHE secp521r1 521 yes 260 low
ECDHE-RSA-AES128-SHA ECDHE x448 448 yes 224 low
ECDHE-RSA-AES128-SHA ECDHE x25519 256 yes 128 low
ECDHE-RSA-AES128-SHA ECDHE secp384r1 384 yes 192 low
ECDHE-RSA-AES128-SHA ECDHE secp256r1 256 yes 128 low
ECDHE-RSA-AES128-SHA ECDHE secp521r1 521 yes 260 low
AECDH-AES256-SHA ECDHA x448 448 yes 224 low
AECDH-AES256-SHA ECDHA x25519 256 yes 128 low
AECDH-AES256-SHA ECDHA secp384r1 384 yes 192 low
AECDH-AES256-SHA ECDHA secp256r1 256 yes 128 low
AECDH-AES256-SHA ECDHA secp521r1 521 yes 260 low
AECDH-AES128-SHA ECDHA x448 448 yes 224 low
AECDH-AES128-SHA ECDHA x25519 256 yes 128 low
AECDH-AES128-SHA ECDHA secp384r1 384 yes 192 low
AECDH-AES128-SHA ECDHA secp256r1 256 yes 128 low
AECDH-AES128-SHA ECDHA secp521r1 521 yes 260 low
TLSv1.3
TLS13-AES-128-GCM-SHA256 ECDHE x25519 256 yes 128 low
TLS13-AES-128-GCM-SHA256 ECDHE x448 448 yes 224 low
TLS13-AES-128-GCM-SHA256 ECDHE secp256r1 256 yes 128 low
TLS13-AES-128-GCM-SHA256 ECDHE secp521r1 521 yes 260 low
TLS13-AES-128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low
TLS13-AES-256-GCM-SHA384 ECDHE x25519 256 yes 128 low
TLS13-AES-256-GCM-SHA384 ECDHE x448 448 yes 224 low
TLS13-AES-256-GCM-SHA384 ECDHE secp256r1 256 yes 128 low
TLS13-AES-256-GCM-SHA384 ECDHE secp521r1 521 yes 260 low
TLS13-AES-256-GCM-SHA384 ECDHE secp384r1 384 yes 192 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE x25519 256 yes 128 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE x448 448 yes 224 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp256r1 256 yes 128 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp521r1 521 yes 260 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp384r1 384 yes 192 low

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	6
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2018-01-04 17:39:37.0

THREAT:
The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

IP address	Host name
185.132.38.51	basil.wingpath.co.uk

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	45006
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2003-05-09 18:28:51.0

THREAT:
Traceroute describes the path in realtime from the scanner to the remote host being contacted. It reports the IP addresses of all the routers in between.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Hops IP Round Trip Time Probe

Port	
1	140.91.222.77 0.27ms ICMP
2	80.249.213.176 0.75ms ICMP
3	80.249.210.180 19.47ms ICMP
4	212.227.117.77 18.59ms ICMP
5	212.227.117.2 24.00ms ICMP
6	212.227.117.200 28.69ms ICMP
7	212.227.120.123 28.80ms ICMP
8	*.*.* 0.00ms Other 80
9	109.228.63.159 27.42ms ICMP
10	185.132.38.51 27.50ms ICMP

Maximum Number of Links Reached During Crawl

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150026
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:46.0

THREAT:
The maximum number of links specified for this scan has been reached. The links crawled to reach this threshold can include requests made via HTML form submissions and links requested in anonymous and authenticated states. Consequently, the list of links crawled (QID 150009) may reflect a lower number than the combination of links and forms requested during the crawl.

IMPACT:
Some links that lead to different areas of the site's functionality may have been missed.

SOLUTION:
Increase the maximum number of links in order to ensure broader coverage of the Web application. It is important to note that increasing the number of links crawled can dramatically increase the time required to test the Web application.

RESULT:
Maximum request count reached: 300

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:

The following is a list of detected SSL/TLS protocol properties.

IMPACT:

- Items include:
- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 - Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 - Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
 - Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
 - Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

RESULT:

NAME STATUS

TLSv1	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client
OCSP stapling	no
SCT extension	no
TLSv1.1	
Extended Master Secret	yes
Encrypt Then MAC	yes
Heartbeat	no
Truncated HMAC	no
Cipher priority controlled by	client


OCSF stapling no
SCT extension no
TLSv1.2
Extended Master Secret yes
Encrypt Then MAC yes
Heartbeat no
Truncated HMAC no
Cipher priority controlled by client
OCSF stapling no
SCT extension no
TLSv1.3
Heartbeat no
Cipher priority controlled by client
OCSF stapling no
SCT extension no

Open TCP Services List

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 82023
Category: TCP/IP
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2024-05-01 12:28:44.0

THREAT:

The port scanner enables unauthorized users with the appropriate tools to draw a map of all services on this host that can be accessed from the Internet. The test was carried out with a "stealth" port scanner so that the server does not log real connections.

The Results section displays the port number (Port), the default service listening on the port (IANA Assigned Ports/Services), the description of the service (Description) and the service that the scanner detected using service discovery (Service Detected).

IMPACT:

Unauthorized users can exploit this information to test vulnerabilities in each of the open services.

SOLUTION:

Shut down any unknown or unused service on the list. If you have difficulty figuring out which service is provided by which process or program, contact your provider's support team. For more information about commercial and open-source Intrusion Detection Systems available for detecting port scanners of this kind, visit the [CERT Web site](#).

RESULT:

Port IANA Assigned Ports/Services Description Service Detected OS On Redirected


Port
22 ssh SSH Remote Login Protocol ssh
25 smtp Simple Mail Transfer smtp
80 www-http World Wide Web HTTP http
443 https http protocol over TLS/SSL http over ssl

Referrer-Policy HTTP Security Header Not Detected port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 48131
Category: Information gathering
CVE ID: -
Vendor Reference: [Referrer-Policy](#)
Bugtraq ID: -
Last Update: 2023-01-18 13:30:16.0

THREAT:

No Referrer Policy is specified for the link. It checks for one of the following Referrer Policy in the response headers:

- 1) no-referrer
- 2) no-referrer-when-downgrade
- 3) same-origin
- 4) origin
- 5) origin-when-cross-origin
- 6) strict-origin
- 7) strict-origin-when-cross-origin

QID Detection Logic(Unauthenticated):

If the Referrer Policy header is not found , checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

IMPACT:

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

SOLUTION:

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:

- <https://www.w3.org/TR/referrer-policy/>
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>

RESULT:

Referrer-Policy HTTP Header missing on 80 port.

GET / HTTP/1.1
Host: wingpath.co.uk
Connection: Keep-Alive

List of Web Directories

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 86672
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2004-09-10 23:40:57.0

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

Directory Source
/admin/ brute force
/bin/ brute force
/js/ brute force
/javascript/ brute force
/modbus/ web page
/js/ web page
/images/ web page
/admin/ web page
/bin/ web page

SSL Certificate - Information

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME VALUE

- (0)CERTIFICATE 0
- (0)Version 3 (0x2)
- (0)Serial Number 04:d6:7d:da:9b:9f:d8:59:74:d3:bd:de:d2:86:52:d7:77:fc
- (0)Signature Algorithm sha256WithRSAEncryption
- (0)ISSUER NAME
 - countryName US
 - organizationName Let's Encrypt
 - commonName R3
- (0)SUBJECT NAME
 - commonName wingpath.co.uk
- (0)Valid From May 9 16:08:39 2024 GMT
- (0)Valid Till Aug 7 16:08:38 2024 GMT
- (0)Public Key Algorithm id-ecPublicKey
- (0)EC Public Key
 - (0) Public-Key: (256 bit)
 - (0) pub:
 - (0) 04:eb:ff:b5:d5:7d:c7:7f:06:0f:87:ec:1a:1a:13:
 - (0) b4:fd:ec:98:93:07:b9:3c:3f:58:f4:8e:67:ed:f9:
 - (0) 48:0d:bd:64:e9:bb:8c:73:bf:b7:15:2d:3a:f4:a1:
 - (0) 28:cc:ae:5b:bd:1a:85:0c:45:37:80:7d:9b:8f:6c:
 - (0) 65:ef:22:4d:83
 - (0) ASN1 OID: prime256v1
 - (0) NIST CURVE: P-256
- (0)X509v3 EXTENSIONS
 - (0)X509v3 Key Usage critical
 - (0) Digital Signature
 - (0)X509v3 Extended Key Usage TLS Web Server Authentication, TLS Web Client Authentication
 - (0)X509v3 Basic Constraints critical
 - (0) CA:FALSE
 - (0)X509v3 Subject Key Identifier D9:27:F4:84:7C:0D:5F:3A:0B:27:47:1C:06:89:8F:05:D2:11:35:16
 - (0)X509v3 Authority Key Identifier keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:

C6

(0)Authority Information Access OCSP - URI:http://r3.o.lencr.org
(0) CA Issuers - URI:http://r3.i.lencr.org/
(0)X509v3 Subject Alternative Name DNS:wingpath.co.uk
(0)X509v3 Certificate Policies Policy: 2.23.140.1.2.1
(0)CT Precertificate SCTs Signed Certificate Timestamp:
(0) Version : v1 (0x0)
(0) Log ID : 3F:17:4B:4F:D7:22:47:58:94:1D:65:1C:84:BE:0D:12:
(0) ED:90:37:7F:1F:85:6A:EB:C1:BF:28:85:EC:F8:64:6E
(0) Timestamp : May 9 17:08:39.282 2024 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:45:02:20:3A:99:83:0E:40:72:04:B4:F5:03:E4:15:
(0) C0:E1:1C:13:0C:37:D9:22:F2:21:C8:D2:78:17:95:7B:
(0) 71:18:47:31:02:21:00:FB:0F:9C:24:9A:13:34:5A:62:
(0) AE:2E:BF:B4:2D:11:1C:08:4C:4E:2E:57:1A:32:83:95:
(0) 94:54:BE:7A:27:A6:69
(0) Signed Certificate Timestamp:
(0) Version : v1 (0x0)
(0) Log ID : EE:CD:D0:64:D5:DB:1A:CE:C5:5C:B7:9D:B4:CD:13:A2:
(0) 32:87:46:7C:BC:EC:DE:C3:51:48:59:46:71:1F:B5:9B
(0) Timestamp : May 9 17:08:39.287 2024 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:44:02:20:13:1D:12:F4:00:FF:8C:6B:6E:00:FD:D5:
(0) 1F:2F:C5:6C:EE:C0:99:6A:C6:D7:0C:CA:6C:91:33:6C:
(0) 6E:A4:56:A1:02:20:79:77:D8:44:66:DD:3B:04:D6:1A:
(0) 90:A1:50:F3:27:B7:A2:51:19:B4:D6:56:D1:E6:4A:3E:
(0) 32:CC:67:B7:38:81
(0)Signature (256 octets)
(0) 01:4f:69:c5:7e:41:9e:11:1a:e5:ac:14:dd:17:9f:1a
(0) 4f:0a:d3:f3:03:13:91:5b:b7:85:1d:8b:ec:8c:01:96
(0) c5:6e:60:de:d5:68:a5:bf:e7:34:67:44:90:d3:f3:17
(0) 94:b1:a3:e0:d6:16:38:a0:c5:2d:d0:e2:c9:8f:1f:d1
(0) 55:c9:1d:aa:ef:fd:77:65:17:0b:26:4e:0b:ed:ba:32
(0) 0e:ea:d3:91:f0:22:25:25:9d:9c:ba:fe:f4:cf:23:99
(0) 7f:bf:95:d7:ea:0a:ea:4f:12:74:66:d1:d2:7d:52:ec
(0) d5:95:83:bc:29:17:dc:02:9c:95:8b:b2:51:da:e9:9b
(0) 89:fe:76:f0:3b:19:1d:c1:01:bc:cd:39:96:8d:fa:8c
(0) ca:c2:f1:cc:2e:64:c7:53:26:86:c7:ba:51:4d:8e:7b
(0) ed:a0:5b:c6:38:ba:bd:98:66:21:cc:aa:e5:26:b9:ee
(0) 27:74:f5:e6:f5:02:f4:6c:ff:ec:44:43:0a:97:91:05
(0) 06:49:b0:3d:32:7f:91:45:13:6e:43:26:65:a3:ff:9b
(0) 39:8f:af:bc:cb:6f:88:b5:64:be:32:b7:36:f3:e7:a0
(0) 11:c9:7f:7a:ca:99:ef:e9:1a:bd:df:b4:9a:96:1c:b4
(0) fd:4c:7e:05:5e:e9:41:3e:6c:17:87:9e:5d:96:f2:d2
(1)CERTIFICATE 1
(1)Version 3 (0x2)
(1)Serial Number 91:2b:08:4a:cf:0c:18:a7:53:f6:d6:2e:25:a7:5f:5a
(1)Signature Algorithm sha256WithRSAEncryption
(1)ISSUER NAME
countryName US
organizationName Internet Security Research Group
commonName ISRG Root X1
(1)SUBJECT NAME
countryName US

organizationName Let's Encrypt
commonName R3
(1)Valid From Sep 4 00:00:00 2020 GMT
(1)Valid Till Sep 15 16:00:00 2025 GMT
(1)Public Key Algorithm rsaEncryption
(1)RSA Public Key (2048 bit)
(1) RSA Public-Key: (2048 bit)
(1) Modulus:
(1) 00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55:
(1) 92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:
(1) 2b:b9:c5:4c:b1:af:8e:6b:f9:75:c8:a3:d7:0f:47:
(1) 94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42:
(1) a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38:
(1) e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa:
(1) 37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52:
(1) 45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de:
(1) 60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b:
(1) d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8:
(1) 30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17:
(1) c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46:
(1) e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7:
(1) a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98:
(1) 09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af:
(1) 63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d:
(1) a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b:
(1) db:15
(1) Exponent: 65537 (0x10001)
(1)X509v3 EXTENSIONS
(1)X509v3 Key Usage critical
(1) Digital Signature, Certificate Sign, CRL Sign
(1)X509v3 Extended Key Usage TLS Web Client Authentication, TLS Web Server Authentication
(1)X509v3 Basic Constraints critical
(1) CA:TRUE, pathlen:0
(1)X509v3 Subject Key Identifier 14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
(1)X509v3 Authority Key Identifier keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
(1)Authority Information Access CA Issuers - URI:<http://x1.i.lencr.org/>
(1)X509v3 CRL Distribution Points
(1) Full Name:
(1) URI:<http://x1.c.lencr.org/>
(1)X509v3 Certificate Policies Policy: 2.23.140.1.2.1
(1) Policy: 1.3.6.1.4.1.44947.1.1.1
(1)Signature (512 octets)
(1) 85:ca:4e:47:3e:a3:f7:85:44:85:bc:d5:67:78:b2:98
(1) 63:ad:75:4d:1e:96:3d:33:65:72:54:2d:81:a0:ea:c3
(1) ed:f8:20:bf:5f:cc:b7:70:00:b7:6e:3b:f6:5e:94:de
(1) e4:20:9f:a6:ef:8b:b2:03:e7:a2:b5:16:3c:91:ce:b4
(1) ed:39:02:e7:7c:25:8a:47:e6:65:6e:3f:46:f4:d9:f0
(1) ce:94:2b:ee:54:ce:12:bc:8c:27:4b:b8:c1:98:2f:a2
(1) af:cd:71:91:4a:08:b7:c8:b8:23:7b:04:2d:08:f9:08
(1) 57:3e:83:d9:04:33:0a:47:21:78:09:82:27:c3:2a:c8
(1) 9b:b9:ce:5c:f2:64:c8:c0:be:79:c0:4f:8e:6d:44:0c
(1) 5e:92:bb:2e:f7:8b:10:e1:e8:1d:44:29:db:59:20:ed
(1) 63:b9:21:f8:12:26:94:93:57:a0:1d:65:04:c1:0a:22
(1) ae:10:0d:43:97:a1:18:1f:7e:e0:e0:86:37:b5:5a:b1
(1) bd:30:bf:87:6e:2b:2a:ff:21:4e:1b:05:c3:f5:18:97
(1) f0:5e:ac:c3:a5:b8:6a:f0:2e:bc:3b:33:b9:ee:4b:de

(1) cc:fc:e4:af:84:0b:86:3f:c0:55:43:36:f6:68:e1:36
(1) 17:6a:8e:99:d1:ff:a5:40:a7:34:b7:c0:d0:63:39:35
(1) 39:75:6e:f2:ba:76:c8:93:02:e9:a9:4b:6c:17:ce:0c
(1) 02:d9:bd:81:fb:9f:b7:68:d4:06:65:b3:82:3d:77:53
(1) f8:8e:79:03:ad:0a:31:07:75:2a:43:d8:55:97:72:c4
(1) 29:0e:f7:c4:5d:4e:c8:ae:46:84:30:d7:f2:85:5f:18
(1) a1:79:bb:e7:5e:70:8b:07:e1:86:93:c3:b9:8f:dc:61
(1) 71:25:2a:af:df:ed:25:50:52:68:8b:92:dc:e5:d6:b5
(1) e3:da:7d:d0:87:6c:84:21:31:ae:82:f5:fb:b9:ab:c8
(1) 89:17:3d:e1:4c:e5:38:0e:f6:bd:2b:bd:96:81:14:eb
(1) d5:db:3d:20:a7:7e:59:d3:e2:f8:58:f9:5b:b8:48:cd
(1) fe:5c:4f:16:29:fe:1e:55:23:af:c8:11:b0:8d:ea:7c
(1) 93:90:17:2f:fd:ac:a2:09:47:46:3f:f0:e9:b0:b7:ff
(1) 28:4d:68:32:d6:67:5e:1e:69:a3:93:b8:f5:9d:8b:2f
(1) 0b:d2:52:43:a6:6f:32:57:65:4d:32:81:df:38:53:85
(1) 5d:7e:5d:66:29:ea:b8:dd:e4:95:b5:cd:b5:56:12:42
(1) cd:c4:4e:c6:25:38:44:50:6d:ec:ce:00:55:18:fe:e9
(1) 49:64:d4:4e:ca:97:9c:b4:5b:c0:73:a8:ab:b8:47:c2
NAME VALUE
(0)CERTIFICATE 0
(0)Version 3 (0x2)
(0)Serial Number 04:8a:11:fa:04:d7:11:8c:1f:8e:32:2b:af:13:fc:37:82:af
(0)Signature Algorithm sha256WithRSAEncryption
(0)ISSUER NAME
countryName US
organizationName Let's Encrypt
commonName R3
(0)SUBJECT NAME
commonName coppermist.co.uk
(0)Valid From May 7 16:07:14 2024 GMT
(0)Valid Till Aug 5 16:07:13 2024 GMT
(0)Public Key Algorithm id-ecPublicKey
(0)EC Public Key
(0) Public-Key: (256 bit)
(0) pub:
(0) 04:00:c1:10:69:b5:45:f9:61:4c:d4:68:34:8d:d9:
(0) 97:e8:2e:b9:3b:24:20:5c:52:ee:10:af:81:fc:7b:
(0) 85:58:57:b1:fd:f4:af:9a:11:ae:bb:4e:88:82:15:
(0) 77:42:bd:08:88:9d:d0:ae:22:f8:49:b6:60:77:43:
(0) cd:91:6e:13:29
(0) ASN1 OID: prime256v1
(0) NIST CURVE: P-256
(0)X509v3 EXTENSIONS
(0)X509v3 Key Usage critical
(0) Digital Signature
(0)X509v3 Extended Key Usage TLS Web Server Authentication, TLS Web Client Authentication
(0)X509v3 Basic Constraints critical
(0) CA:FALSE
(0)X509v3 Subject Key Identifier E1:06:F9:05:30:88:00:99:07:D5:76:9C:0B:61:63:B7:81:C8:56:A3
(0)X509v3 Authority Key Identifier keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:
C6
(0)Authority Information Access OCSP - URI:http://r3.o.lencr.org
(0) CA Issuers - URI:http://r3.i.lencr.org/
(0)X509v3 Subject Alternative Name DNS:coppermist.co.uk
(0)X509v3 Certificate Policies Policy: 2.23.140.1.2.1
(0)CT Precertificate SCTs Signed Certificate Timestamp:

(0) Version : v1 (0x0)
(0) Log ID : 19:98:10:71:09:F0:D6:52:2E:30:80:D2:9E:3F:64:BB:
(0) 83:6E:28:CC:F9:0F:52:8E:EE:DF:CE:4A:3F:16:B4:CA
(0) Timestamp : May 7 17:07:14.854 2024 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:46:02:21:00:90:BC:54:4A:D7:B9:DB:2B:64:7E:6F:
(0) DE:D1:5A:61:33:08:B3:30:88:40:47:9C:B3:9B:43:AB:
(0) 56:D7:6F:92:03:02:21:00:CF:40:65:9A:FC:4B:3E:47:
(0) 0B:CE:4E:D2:98:BD:45:CC:8E:17:2D:BD:E5:0B:B6:DD:
(0) 3F:79:F2:35:0F:A8:C5:B4
(0) Signed Certificate Timestamp:
(0) Version : v1 (0x0)
(0) Log ID : 3F:17:4B:4F:D7:22:47:58:94:1D:65:1C:84:BE:0D:12:
(0) ED:90:37:7F:1F:85:6A:EB:C1:BF:28:85:EC:F8:64:6E
(0) Timestamp : May 7 17:07:14.851 2024 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:46:02:21:00:ED:84:56:86:42:08:9C:18:4C:C7:2A:
(0) 14:D9:96:22:43:80:5E:CF:F6:F9:55:4B:E2:BC:52:E5:
(0) AC:39:1E:37:EE:02:21:00:D4:A2:E8:DA:A4:1F:5B:A3:
(0) 75:0B:29:FB:5F:8A:94:EA:2E:49:49:71:90:D0:76:42:
(0) 5A:3E:74:2F:9E:C8:00:08
(0)Signature (256 octets)
(0) a1:19:d7:86:50:16:e1:de:9d:97:53:60:8e:ea:93:04
(0) 3c:03:62:bf:ea:d3:e8:a8:e6:5d:4b:1a:70:5b:a6:3a
(0) 21:74:45:27:da:0d:aa:6f:71:f4:f4:14:a6:13:6f:da
(0) 7d:ad:ff:22:ad:f2:c5:1b:2a:85:b0:ef:cc:44:be:29
(0) 09:39:7e:0d:ac:7e:a2:d7:a3:05:0b:d2:e0:9c:91:97
(0) 50:dd:16:92:42:f9:30:39:22:4c:c9:43:4e:13:0c:01
(0) e0:0a:80:14:24:80:96:2c:69:8c:af:82:57:3e:93:78
(0) 29:5b:bb:21:63:a6:5c:84:b6:0d:c5:22:83:9d:33:70
(0) 02:5c:8c:44:42:29:b6:69:5c:cd:e4:69:f4:1e:c4:32
(0) ee:9a:9d:94:af:57:51:27:01:c8:73:11:49:4c:f2:c3
(0) df:e8:a9:4b:94:32:71:d6:7c:63:f6:95:64:dc:58:fd
(0) 05:9e:b4:3d:ad:a0:35:66:65:32:57:07:4d:cf:64:b5
(0) 17:0f:53:12:49:ce:22:b9:cc:2f:21:62:d1:c0:88:80
(0) e2:25:be:4a:e9:a1:86:79:70:b3:e0:bd:2b:84:ec:f5
(0) cb:20:f3:e6:6a:e8:c5:99:e6:7c:e0:91:21:c9:41:a6
(0) 43:ed:74:1a:56:1b:29:ad:62:bf:75:ab:17:82:6f:4f
(1)CERTIFICATE 1
(1)Version 3 (0x2)
(1)Serial Number 91:2b:08:4a:cf:0c:18:a7:53:f6:d6:2e:25:a7:5f:5a
(1)Signature Algorithm sha256WithRSAEncryption
(1)ISSUER NAME
countryName US
organizationName Internet Security Research Group
commonName ISRG Root X1
(1)SUBJECT NAME
countryName US
organizationName Let's Encrypt
commonName R3
(1)Valid From Sep 4 00:00:00 2020 GMT
(1)Valid Till Sep 15 16:00:00 2025 GMT
(1)Public Key Algorithm rsaEncryption
(1)RSA Public Key (2048 bit)

(1) RSA Public-Key: (2048 bit)

(1) Modulus:

(1) 00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55:

(1) 92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:

(1) 2b:b9:c5:4c:b1:af:8e:6b:f9:75:c8:a3:d7:0f:47:

(1) 94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42:

(1) a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38:

(1) e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa:

(1) 37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52:

(1) 45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de:

(1) 60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b:

(1) d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8:

(1) 30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17:

(1) c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46:

(1) e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7:

(1) a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98:

(1) 09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af:

(1) 63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d:

(1) a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b:

(1) db:15

(1) Exponent: 65537 (0x10001)

(1)X509v3 EXTENSIONS

(1)X509v3 Key Usage critical

(1) Digital Signature, Certificate Sign, CRL Sign

(1)X509v3 Extended Key Usage TLS Web Client Authentication, TLS Web Server Authentication

(1)X509v3 Basic Constraints critical

(1) CA:TRUE, pathlen:0

(1)X509v3 Subject Key Identifier 14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6

(1)X509v3 Authority Key Identifier keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E

(1)Authority Information Access CA Issuers - URI:<http://x1.i.lencr.org/>

(1)X509v3 CRL Distribution Points

(1) Full Name:

(1) URI:<http://x1.c.lencr.org/>

(1)X509v3 Certificate Policies Policy: 2.23.140.1.2.1

(1) Policy: 1.3.6.1.4.1.44947.1.1.1

(1)Signature (512 octets)

(1) 85:ca:4e:47:3e:a3:f7:85:44:85:bc:d5:67:78:b2:98

(1) 63:ad:75:4d:1e:96:3d:33:65:72:54:2d:81:a0:ea:c3

(1) ed:f8:20:bf:5f:cc:b7:70:00:b7:6e:3b:f6:5e:94:de

(1) e4:20:9f:a6:ef:8b:b2:03:e7:a2:b5:16:3c:91:ce:b4

(1) ed:39:02:e7:7c:25:8a:47:e6:65:6e:3f:46:f4:d9:f0

(1) ce:94:2b:ee:54:ce:12:bc:8c:27:4b:b8:c1:98:2f:a2

(1) af:cd:71:91:4a:08:b7:c8:b8:23:7b:04:2d:08:f9:08

(1) 57:3e:83:d9:04:33:0a:47:21:78:09:82:27:c3:2a:c8

(1) 9b:b9:ce:5c:f2:64:c8:c0:be:79:c0:4f:8e:6d:44:0c

(1) 5e:92:bb:2e:f7:8b:10:e1:e8:1d:44:29:db:59:20:ed

(1) 63:b9:21:f8:12:26:94:93:57:a0:1d:65:04:c1:0a:22

(1) ae:10:0d:43:97:a1:18:1f:7e:e0:e0:86:37:b5:5a:b1

(1) bd:30:bf:87:6e:2b:2a:ff:21:4e:1b:05:c3:f5:18:97

(1) f0:5e:ac:c3:a5:b8:6a:f0:2e:bc:3b:33:b9:ee:4b:de

(1) cc:fc:e4:af:84:0b:86:3f:c0:55:43:36:f6:68:e1:36

(1) 17:6a:8e:99:d1:ff:a5:40:a7:34:b7:c0:d0:63:39:35

(1) 39:75:6e:f2:ba:76:c8:93:02:e9:a9:4b:6c:17:ce:0c

(1) 02:d9:bd:81:fb:9f:b7:68:d4:06:65:b3:82:3d:77:53

(1) f8:8e:79:03:ad:0a:31:07:75:2a:43:d8:55:97:72:c4

(1) 29:0e:f7:c4:5d:4e:c8:ae:46:84:30:d7:f2:85:5f:18

(1) a1:79:bb:e7:5e:70:8b:07:e1:86:93:c3:b9:8f:dc:61
(1) 71:25:2a:af:df:ed:25:50:52:68:8b:92:dc:e5:d6:b5
(1) e3:da:7d:d0:87:6c:84:21:31:ae:82:f5:fb:b9:ab:c8
(1) 89:17:3d:e1:4c:e5:38:0e:f6:bd:2b:bd:96:81:14:eb
(1) d5:db:3d:20:a7:7e:59:d3:e2:f8:58:f9:5b:b8:48:cd
(1) fe:5c:4f:16:29:fe:1e:55:23:af:c8:11:b0:8d:ea:7c
(1) 93:90:17:2f:fd:ac:a2:09:47:46:3f:f0:e9:b0:b7:ff
(1) 28:4d:68:32:d6:67:5e:1e:69:a3:93:b8:f5:9d:8b:2f
(1) 0b:d2:52:43:a6:6f:32:57:65:4d:32:81:df:38:53:85
(1) 5d:7e:5d:66:29:ea:b8:dd:e4:95:b5:cd:b5:56:12:42
(1) cd:c4:4e:c6:25:38:44:50:6d:ec:ce:00:55:18:fe:e9
(1) 49:64:d4:4e:ca:97:9c:b4:5b:c0:73:a8:ab:b8:47:c2

SSL Server default Diffie-Hellman prime information

port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38609
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2015-05-26 22:09:34.0

THREAT:
Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS. - For fixed primes: 1024 and below are considered unsafe. - For variable primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
SSL server default to use Diffie-Hellman key exchange method with variable 2048(bits) prime

SSL Certificate - Information

port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	86002
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-07 22:23:33.0

THREAT:
SSL certificate information is provided in the Results section.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

NAME	VALUE
(0)CERTIFICATE 0	
(0)Version 3 (0x2)	
(0)Serial Number 26:ec:8d:dc:ff:05:a1:ca:a4:d5:e1:c4:93:da:a7:38:17:b6:40:b0	
(0)Signature Algorithm sha256WithRSAEncryption	
(0)ISSUER NAME	commonName localhost.localdomain
(0)SUBJECT NAME	commonName localhost.localdomain
(0)Valid From Apr 14 08:20:21 2021 GMT	
(0)Valid Till Apr 12 08:20:21 2031 GMT	
(0)Public Key Algorithm rsaEncryption	
(0)RSA Public Key (2048 bit)	
(0) RSA Public-Key: (2048 bit)	
(0) Modulus:	
(0) 00:a5:1b:8b:bc:ad:07:86:a1:95:0b:c8:9e:97:91:	
(0) 1b:0a:1e:ff:d3:a7:1c:8a:f2:b3:90:3e:35:56:f5:	
(0) 4a:f6:3b:3d:e0:06:d9:00:ac:c2:94:21:c3:ba:87:	
(0) 4e:09:d0:2a:d6:46:6d:06:6b:98:49:0d:74:f4:59:	
(0) 8d:b6:7e:f9:05:5f:c6:5f:31:d5:8a:df:82:70:c9:	
(0) 20:ba:69:3f:09:0a:7d:82:5b:7d:59:4c:5e:49:5a:	
(0) c5:07:63:79:59:56:20:73:26:b0:90:02:c0:56:67:	
(0) 80:1d:b3:24:fb:d9:b1:d3:a3:e6:7c:31:57:c8:f6:	
(0) bc:b0:2d:73:6c:39:74:50:20:85:a9:ee:cc:ae:5b:	
(0) 45:a1:0b:a1:df:f7:62:16:3a:70:4b:f4:fb:7e:46:	
(0) fe:5b:a3:52:2e:9f:fc:91:f4:31:02:2e:cf:46:4b:	
(0) 8f:be:d9:22:76:68:6b:36:ae:f4:f6:fb:b1:a0:3b:	
(0) bb:a6:71:17:51:8d:dd:21:c8:e4:27:66:fe:c1:78:	
(0) 50:cd:5a:81:ea:bd:c8:3a:ef:24:dd:96:c7:ec:36:	
(0) e8:fa:74:6b:e2:f4:a3:e7:b7:d8:29:c4:8c:78:3d:	
(0) 9b:43:75:71:c0:38:3c:76:9a:0a:8f:30:c8:16:9f:	

(0) 82:a9:31:ad:25:5c:bb:0e:f3:91:fe:70:9d:a8:55:
(0) 79:b7
(0) Exponent: 65537 (0x10001)
(0)X509v3 EXTENSIONS
(0)X509v3 Basic Constraints CA:FALSE
(0)X509v3 Subject Alternative Name DNS:localhost.localdomain
(0)Signature (256 octets)
(0) 89:f0:b5:80:73:7f:da:1c:41:5c:7e:65:5f:fd:08:e2
(0) c0:66:20:22:26:d0:07:9d:ba:3b:41:5f:17:77:72:d4
(0) 3b:3c:80:a4:9a:20:fd:f5:9c:1b:1b:4a:e4:47:b3:29
(0) 53:cf:7b:95:10:b9:a4:f1:e5:2a:0f:b6:23:3b:28:c3
(0) 00:86:76:45:ec:cc:46:2b:24:48:f4:4d:c8:00:98:9b
(0) cf:31:ff:63:0a:cb:ab:5d:ae:f5:01:81:5a:de:41:b2
(0) 32:d8:39:1a:77:5d:cd:ed:e7:45:ce:8a:cf:99:0f:b8
(0) 5e:bf:4f:de:92:2f:ee:26:a6:3c:39:0d:d3:41:4d:be
(0) 7c:7e:32:0f:5d:8d:6d:c8:85:74:80:5a:df:80:dc:ef
(0) 69:2e:31:a0:e0:5a:68:06:5b:1e:8f:40:42:1a:48:74
(0) 7a:53:d6:17:7b:89:b5:8b:e4:28:05:fc:70:f3:37:04
(0) 92:de:d1:a2:c8:f2:e6:37:1a:b6:d4:14:6e:26:c1:be
(0) 91:2e:e8:cf:fa:cc:5c:78:19:90:b5:17:f1:25:99:58
(0) 2b:fd:f6:ef:a3:9d:a8:76:88:0e:4c:57:1c:04:eb:7e
(0) cd:4c:cb:ae:75:2c:66:2d:70:ed:9f:82:53:aa:d4:75
(0) 18:00:66:dd:73:bf:0c:bd:d1:e3:5d:81:16:bb:37:9d

Web Server Version

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	86000
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-12-20 13:32:52.0

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Apache/2.4.41 (Ubuntu)

Default Web Page (Follow HTTP Redirection)port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 13910
Category: CGI
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2020-11-05 13:13:22.0

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:
[nas-201911-01](#)

RESULT:
GET / HTTP/1.1
Host: wingpath.co.uk
Connection: Keep-Alive

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>421 Misdirected Request</title>
</head><body>
<h1>Misdirected Request</h1>
<p>The client needs a new connection for this
request as the requested host name does not match
the Server Name Indication (SNI) in use for this
connection.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at wingpath.co.uk Port 443</address>
</body></html>
GET / HTTP/1.1
Host: basil.wingpath.co.uk
```

Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 16 May 2024 11:01:51 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT
ETag: "2aa6-5f040bdba30ce"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
Modified from the Debian original for Ubuntu
Last updated: 2016-11-16
See: https://launchpad.net/bugs/1288690
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Ubuntu Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-serif;
font-size: 11pt;
text-align: center;
}

div.main_page {
position: relative;
display: table;

width: 800px;

margin-bottom: 3px;
margin-left: auto;
margin-right: auto;
padding: 0px 0px 0px 0px;

border-width: 2px;
border-color: #212738;
```


border-style: solid;

background-color: #FFFFFF;

text-align: center;
}

div.page_header {
height: 99px;
width: 100%;

background-color: #F5F6F7;
}

div.page_header span {
margin: 15px 0px 0px 50px;

font-size: 180%;
font-weight: bold;
}

div.page_header img {
margin: 3px 0px 0px 40px;

border: 0px 0px 0px;
}

div.table_of_contents {
clear: left;

min-width: 200px;

margin: 3px 3px 3px 3px;

background-color: #FFFFFF;

text-align: left;
}

div.table_of_contents_item {
clear: left;

width: 100%;

margin: 4px 0px 0px 0px;

background-color: #FFFFFF;

color: #000000;
text-align: left;
}

div.table_of_contents_item a {
margin: 6px 0px 0px 6px;
}

```
div.content_section {  
margin: 3px 3px 3px 3px;
```

```
background-color: #FFFFFF;
```

```
text-align: left;  
}
```

```
div.content_section_text {  
padding: 4px 8px 4px 8px;
```

```
color: #000000;  
font-size: 100%;  
}
```

```
div.content_section_text pre {  
margin: 8px 0px 8px 0px;  
padding: 8px 8px 8px 8px;
```

```
border-width: 1px;  
border-style: dotted;  
border-color: #000000;
```

```
background-color: #F5F6F7;
```

```
font-style: italic;  
}
```

```
div.content_section_text p {  
margin-bottom: 6px;  
}
```

```
div.content_section_text ul, div.content_section_text li {  
padding: 4px 8px 4px 16px;  
}
```

```
div.section_header {  
padding: 3px 6px 3px 6px;
```

```
background-color: #8E9CB2;
```

```
color: #FFFFFF;  
font-weight: bold;  
font-size: 112%;  
text-align: center;  
}
```

```
div.section_header_red {  
background-color: #CD214F;  
}
```

```
div.section_header_grey {  
background-color: #9F9386;  
}
```

```
.floating_element {
```

```
position: relative;
float: left;
}

div.table_of_contents_item a,
div.content_section_text a {
text-decoration: none;
font-weight: bold;
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
color: #000000;
}

div.table_of_contents_item a:hover {
background-color: #000000;

color: #FFFFFF;
}

div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
background-color: #DCDFE6;

color: #000000;
}

div.content_section_text a:hover {
background-color: #000000;

color: #DCDFE6;
}

div.validator {
}
</style>
</head>
<body>
<div class="main_page">
<div class="page_header floating_element">

<span class="floating_element">
Apache2 Ubuntu Default Page
</span>
</div>
<!-- <div class="table_of_contents floating_element">
<div class="section_header section_header_grey">
TABLE OF CONTENTS
</div>
<div class="table_of_contents_item floating_element">
<a href="#about">About</a>
</div>
<div class="table_of_contents_item floating_element">
```

```
<a href="#changes">Changes</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#scope">Scope</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#files">Config files</a>
</div>
</div>
-->
<div class="content_section floating_element">

<div class="section_header section_header_red">
<div id="about"></div>
It works!
</div>
<div class="content_section_text">
<p>
This is the default welcome page used to test the correct
operation of the Apache2 server after installation on Ubuntu systems.
It is based on the equivalent page on Debian, from which the Ubuntu Apache
packaging is derived.
If you can read this page, it means that the Apache HTTP server installed at
this site is working properly. You should <b>replace this file</b> (located at
<tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
</p>

<p>
If you are a normal user of this web site and don't know what this page is
about, this probably means that the site is currently unavailable due to
maintenance.
If the problem persists, please contact the site's administrator.
</p>

</div>
<div class="section_header">
<div id="changes"></div>
Configuration Overview
</div>
<div class="content_section_text">
<p>
Ubuntu's Apache2 default configuration is different from the
upstream default configuration, and split into several files optimized for
interaction with Ubuntu tools. The configuration system is
<b>fully documented in
/usr/share/doc/apache2/README.Debian.gz</b>. Refer to this for the full
documentation. Documentation for the web server itself can be
found by accessing the <a href="/manual">manual</a> if the <tt>apache2-doc</tt>
package was installed on this server.

</p>
<p>
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:
</p>
```

```
<pre>
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
</pre>
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled`, `conf-enabled` and `sites-enabled` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers

```
<tt>
a2enmod,
a2dismod,
</tt>
<tt>
a2ensite,
a2dissite,
</tt>
and
<tt>
a2enconf,
a2disconf
</tt>
```

See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`.

Calling `/usr/bin/apache2` directly will not work with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to any file apart of those located in `/var/www`, [public_html](http://httpd.apache.org/docs/2.4/mod/mod_userdir.html) directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

The default Ubuntu document root is `/var/www/html`. You can make your own virtual hosts under `/var/www`. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the `ubuntu-bug` tool to report bugs in the Apache2 package with Ubuntu. However, check [existing bug reports](https://bugs.launchpad.net/ubuntu/+source/apache2) before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.

Web Server Supports HTTP Request Pipelining

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	86565
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2005-02-23 00:25:38.0

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in [this paper by Daniel Roelker](#), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:
N/A

RESULT:
GET / HTTP/1.1
Host:185.132.38.51:80

GET /Q_Evasive/ HTTP/1.1
Host:185.132.38.51:80

HTTP/1.1 404 Not Found
Date: Thu, 16 May 2024 10:39:16 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 275
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at 185.132.38.51 Port 80</address>
</body></html>
```

HTTP/1.1 404 Not Found
Date: Thu, 16 May 2024 10:39:16 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 275
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at 185.132.38.51 Port 80</address>
</body></html>
```

GET / HTTP/1.1
Host:185.132.38.51:80

GET /Q_Evasive/ HTTP/1.1
Host:185.132.38.51:80

HTTP/1.1 404 Not Found
Date: Thu, 16 May 2024 10:39:21 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 275
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at 185.132.38.51 Port 80</address>
</body></html>
```

HTTP/1.1 404 Not Found
Date: Thu, 16 May 2024 10:39:21 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 275
Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at 185.132.38.51 Port 80</address>
</body></html>
```


Web Server Version

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2021-12-20 13:32:52.0

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Apache/2.4.41 (Ubuntu)

Links Rejected By Crawl Scope or Exclusion List

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 150020
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2022-02-07 16:48:28.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:

(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:

https://bugs.launchpad.net/ubuntu/+source/apache2
http://httpd.apache.org/docs/2.4/mod/mod_userdir.html

IP based excluded links:

Profanity Detected in Website Content

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150865
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-04-18 08:20:00.0

THREAT:

Use of profanity or abusive language was discovered during the scan.

IMPACT:

The presence of such language may violate acceptable use policies, community guidelines, or regulatory requirements.

SOLUTION:

Customers are advised to review and address the content to ensure compliance and maintain the integrity of the platform.

RESULT:

Request: https://wingpath.co.uk/docs/modsnmp/troubleshoot.html
Matched Text: he message and press the space bar).
</p>
<div class="section">
<div class="titlepage"><div><div><h3 class="title">
1.SNMP</h3></div></div></div>

```
<p></p>
<p class="troublehead"><a name="SN002"></a>"Unknown host: XXX"</p>
<p>The host name that you entered could not be mapped to an IP address.
</p>
<div class="itemizedlist"><ul class="itemizedlist" style="list-style-type: disc; ">
<li class="listitem"><p>
The address of the <a class="link" href="sn
Comment: Profanity Detected in Website Content at PORT: 443
```

HTTP Response Method and Header Information Collected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP header and method information collected on port 80.

GET / HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

HTTP/1.1 404 Not Found
Date: Thu, 16 May 2024 10:13:39 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 282
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

HTTP Response Method and Header Information Collected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP header and method information collected on port 80.

GET / HTTP/1.1
Host: wingpath.co.uk
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Date: Thu, 16 May 2024 10:27:36 GMT
Server: Apache/2.4.41 (Ubuntu)
Location: https://wingpath.co.uk/
Content-Length: 311
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1


Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 38597

Category: General remote services

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2021-07-12 23:14:58.0

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:


my version target
version
0304 0303
0399 0303
0400 0303
0499 0303

HTTP Public-Key-Pins Security Header Not Detected port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 48002

Category: Information gathering

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2021-07-12 15:16:39.0

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

SSL Server Information Retrieval

port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-05-24 21:02:48.0

THREAT:
The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE

SSLv2 PROTOCOL IS DISABLED
SSLv3 PROTOCOL IS DISABLED
TLSv1 PROTOCOL IS ENABLED
TLSv1 COMPRESSION METHOD None
AES128-SHA RSA RSA SHA1 AES(128) MEDIUM

DHE-RSA-AES128-SHA DH RSA SHA1 AES(128) MEDIUM
ADH-AES128-SHA DH None SHA1 AES(128) MEDIUM
AES256-SHA RSA RSA SHA1 AES(256) HIGH
DHE-RSA-AES256-SHA DH RSA SHA1 AES(256) HIGH
ADH-AES256-SHA DH None SHA1 AES(256) HIGH
CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM
DHE-RSA-CAMELLIA128-SHA DH RSA SHA1 Camellia(128) MEDIUM
ADH-CAMELLIA128-SHA DH None SHA1 Camellia(128) MEDIUM
CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH
DHE-RSA-CAMELLIA256-SHA DH RSA SHA1 Camellia(256) HIGH
ADH-CAMELLIA256-SHA DH None SHA1 Camellia(256) HIGH
SEED-SHA RSA RSA SHA1 SEED(128) MEDIUM
DHE-RSA-SEED-SHA DH RSA SHA1 SEED(128) MEDIUM
ADH-SEED-SHA DH None SHA1 SEED(128) MEDIUM
ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES(128) MEDIUM
ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) HIGH
AECDH-AES128-SHA ECDH None SHA1 AES(128) MEDIUM
AECDH-AES256-SHA ECDH None SHA1 AES(256) HIGH
TLSv1.1 PROTOCOL IS ENABLED
TLSv1.1 COMPRESSION METHOD None
AES128-SHA RSA RSA SHA1 AES(128) MEDIUM
DHE-RSA-AES128-SHA DH RSA SHA1 AES(128) MEDIUM
ADH-AES128-SHA DH None SHA1 AES(128) MEDIUM
AES256-SHA RSA RSA SHA1 AES(256) HIGH
DHE-RSA-AES256-SHA DH RSA SHA1 AES(256) HIGH
ADH-AES256-SHA DH None SHA1 AES(256) HIGH
CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM
DHE-RSA-CAMELLIA128-SHA DH RSA SHA1 Camellia(128) MEDIUM
ADH-CAMELLIA128-SHA DH None SHA1 Camellia(128) MEDIUM
CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH
DHE-RSA-CAMELLIA256-SHA DH RSA SHA1 Camellia(256) HIGH
ADH-CAMELLIA256-SHA DH None SHA1 Camellia(256) HIGH
SEED-SHA RSA RSA SHA1 SEED(128) MEDIUM
DHE-RSA-SEED-SHA DH RSA SHA1 SEED(128) MEDIUM
ADH-SEED-SHA DH None SHA1 SEED(128) MEDIUM
ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES(128) MEDIUM
ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) HIGH
AECDH-AES128-SHA ECDH None SHA1 AES(128) MEDIUM
AECDH-AES256-SHA ECDH None SHA1 AES(256) HIGH
TLSv1.2 PROTOCOL IS ENABLED
TLSv1.2 COMPRESSION METHOD None
AES128-SHA RSA RSA SHA1 AES(128) MEDIUM
DHE-RSA-AES128-SHA DH RSA SHA1 AES(128) MEDIUM
ADH-AES128-SHA DH None SHA1 AES(128) MEDIUM
AES256-SHA RSA RSA SHA1 AES(256) HIGH
DHE-RSA-AES256-SHA DH RSA SHA1 AES(256) HIGH
ADH-AES256-SHA DH None SHA1 AES(256) HIGH
CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM
DHE-RSA-CAMELLIA128-SHA DH RSA SHA1 Camellia(128) MEDIUM
ADH-CAMELLIA128-SHA DH None SHA1 Camellia(128) MEDIUM
DHE-RSA-AES128-SHA256 DH RSA SHA256 AES(128) MEDIUM
DHE-RSA-AES256-SHA256 DH RSA SHA256 AES(256) HIGH
ADH-AES128-SHA256 DH None SHA256 AES(128) MEDIUM
ADH-AES256-SHA256 DH None SHA256 AES(256) HIGH
CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH
DHE-RSA-CAMELLIA256-SHA DH RSA SHA1 Camellia(256) HIGH

ADH-CAMELLIA256-SHA DH None SHA1 Camellia(256) HIGH
SEED-SHA RSA RSA SHA1 SEED(128) MEDIUM
DHE-RSA-SEED-SHA DH RSA SHA1 SEED(128) MEDIUM
ADH-SEED-SHA DH None SHA1 SEED(128) MEDIUM
AES128-GCM-SHA256 RSA RSA AEAD AESGCM(128) MEDIUM
AES256-GCM-SHA384 RSA RSA AEAD AESGCM(256) HIGH
DHE-RSA-AES128-GCM-SHA256 DH RSA AEAD AESGCM(128) MEDIUM
DHE-RSA-AES256-GCM-SHA384 DH RSA AEAD AESGCM(256) HIGH
ADH-AES128-GCM-SHA256 DH None AEAD AESGCM(128) MEDIUM
ADH-AES256-GCM-SHA384 DH None AEAD AESGCM(256) HIGH
CAMELLIA128-SHA256 RSA RSA SHA256 Camellia(128) MEDIUM
DHE-RSA-CAMELLIA128-SHA256 DH RSA SHA256 Camellia(128) MEDIUM
ADH-CAMELLIA128-SHA256 DH None SHA256 Camellia(128) MEDIUM
CAMELLIA256-SHA256 RSA RSA SHA256 Camellia(256) HIGH
DHE-RSA-CAMELLIA256-SHA256 DH RSA SHA256 Camellia(256) HIGH
ADH-CAMELLIA256-SHA256 DH None SHA256 Camellia(256) HIGH
ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES(128) MEDIUM
ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) HIGH
AECDH-AES128-SHA ECDH None SHA1 AES(128) MEDIUM
AECDH-AES256-SHA ECDH None SHA1 AES(256) HIGH
ECDHE-RSA-AES128-SHA256 ECDH RSA SHA256 AES(128) MEDIUM
ECDHE-RSA-AES256-SHA384 ECDH RSA SHA384 AES(256) HIGH
ECDHE-RSA-AES128-GCM-SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM
ECDHE-RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH
ARIA128-GCM-SHA256 RSA RSA AEAD ARIAGCM(128) MEDIUM
ARIA256-GCM-SHA384 RSA RSA AEAD ARIAGCM(256) HIGH
DHE-RSA-ARIA128-GCM-SHA256 DH RSA AEAD ARIAGCM(128) MEDIUM
DHE-RSA-ARIA256-GCM-SHA384 DH RSA AEAD ARIAGCM(256) HIGH
ECDHE-RSA-ARIA128-GCM-SHA256 ECDH RSA AEAD ARIAGCM(128) MEDIUM
ECDHE-RSA-ARIA256-GCM-SHA384 ECDH RSA AEAD ARIAGCM(256) HIGH
ECDHE-RSA-CAMELLIA128-SHA256 ECDH RSA SHA256 Camellia(128) MEDIUM
ECDHE-RSA-CAMELLIA256-SHA384 ECDH RSA SHA384 Camellia(256) HIGH
AES128-CCM RSA RSA AEAD AESCCM(128) MEDIUM
AES256-CCM RSA RSA AEAD AESCCM(256) HIGH
DHE-RSA-AES128-CCM DH RSA AEAD AESCCM(128) MEDIUM
DHE-RSA-AES256-CCM DH RSA AEAD AESCCM(256) HIGH
AES128-CCM-8 RSA RSA AEAD AESCCM8(128) MEDIUM
AES256-CCM-8 RSA RSA AEAD AESCCM8(256) HIGH
DHE-RSA-AES128-CCM-8 DH RSA AEAD AESCCM8(128) MEDIUM
DHE-RSA-AES256-CCM-8 DH RSA AEAD AESCCM8(256) HIGH
ECDHE-RSA-CHACHA20-POLY1305 ECDH RSA AEAD CHACHA20/POLY1305(256) HIGH
DHE-RSA-CHACHA20-POLY1305 DH RSA AEAD CHACHA20/POLY1305(256) HIGH
AES128-SHA256 RSA RSA SHA256 AES(128) MEDIUM
AES256-SHA256 RSA RSA SHA256 AES(256) HIGH
TLSv1.3 PROTOCOL IS ENABLED
TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(128) MEDIUM
TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH
TLS13-CHACHA20-POLY1305-SHA256 N/A N/A AEAD CHACHA20/POLY1305(256) HIGH

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	45039
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-08-27 03:28:53.0

THREAT:
The following host names were discovered for this computer using various methods such as DNS look up, NetBIOS query, and SQL server name query.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Host Name Source
basil.wingpath.co.uk
FQDN

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	45005
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2013-09-27 19:31:33.0

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may aid in launching further attacks against it.

SOLUTION:
N/A

RESULT:
The ISP network handle is: IONOS-NET
ISP Network description:
1&1 IONOS SE

SSL Session Caching Information

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38291
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-03-19 22:48:23.0

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is enabled on the target.

Cookies Collected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150028
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:46:27.0

THREAT:
The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:
Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:
Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:
Total cookies: 1
uid=5075788680; expires=Fri May 16 10:24:32 2025; path=/; domain=wingpath.co.uk; max-age=31535978

Links Rejected By Crawl Scope or Exclusion List port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-02-07 16:48:28.0

THREAT:
One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:

(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:

<https://www.facebook.com/wingpath>

<https://www.americanexpress.com/>

<https://www.se.com/>

<https://twitter.com/WingpathUK>

<http://www.paessler.com/tools/mibimporter>

<http://www.paypal.com/>

<http://modbus.control.com/>

<http://www.modbus.org/>

<http://www.mastercard.com/>

<http://www.emersonprocess.com/>

IP based excluded links:


Links rejected during the test phase not reported due to volume of links.

Host Scan Time - Scanner

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 
QID:	45038
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-09-15 18:02:52.0

THREAT:

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Scan duration: 5557 seconds

Start time: Thu, May 16 2024, 10:09:22 GMT

End time: Thu, May 16 2024, 11:41:59 GMT

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38704
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2023-02-01 23:14:33.0

THREAT:

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

CIPHER NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH

TLSv1.2				
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	x448	448	yes 224 low
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	x25519	256	yes 128 low
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	secp384r1	384	yes 192 low
ECDHE-ECDSA-AES256-GCM-SHA384	ECDHE	secp256r1	256	yes 128 low
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	x448	448	yes 224 low
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	x25519	256	yes 128 low
ECDHE-ECDSA-CHACHA20-POLY1305	ECDHE	secp384r1	384	yes 192 low

ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE secp256r1 256 yes 128 low
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE x448 448 yes 224 low
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE x25519 256 yes 128 low
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low
ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE secp256r1 256 yes 128 low
TLSv1.3
TLS13-AES-128-GCM-SHA256 ECDHE x25519 256 yes 128 low
TLS13-AES-128-GCM-SHA256 ECDHE secp256r1 256 yes 128 low
TLS13-AES-128-GCM-SHA256 ECDHE x448 448 yes 224 low
TLS13-AES-128-GCM-SHA256 ECDHE secp521r1 521 yes 260 low
TLS13-AES-128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low
TLS13-AES-256-GCM-SHA384 ECDHE x25519 256 yes 128 low
TLS13-AES-256-GCM-SHA384 ECDHE secp256r1 256 yes 128 low
TLS13-AES-256-GCM-SHA384 ECDHE x448 448 yes 224 low
TLS13-AES-256-GCM-SHA384 ECDHE secp521r1 521 yes 260 low
TLS13-AES-256-GCM-SHA384 ECDHE secp384r1 384 yes 192 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE x25519 256 yes 128 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp256r1 256 yes 128 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE x448 448 yes 224 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp521r1 521 yes 260 low
TLS13-CHACHA20-POLY1305-SHA256 ECDHE secp384r1 384 yes 192 low

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38706
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-09 04:32:38.0

THREAT:
The following is a list of detected SSL/TLS protocol properties.

IMPACT:
Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2

- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

SOLUTION:

N/A

RESULT:

NAME STATUS

TLSv1.2
Extended Master Secret yes
Heartbeat no
Cipher priority controlled by client
OCSP stapling no
SCT extension no
TLSv1.3
Heartbeat no
Cipher priority controlled by client
OCSP stapling no
SCT extension no

Maximum Number of Links Reached During Crawlport 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 150026
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2009-01-16 18:02:46.0

THREAT:

The maximum number of links specified for this scan has been reached. The links crawled to reach this threshold can include requests made via HTML form submissions and links requested in anonymous and authenticated states. Consequently, the list of links crawled (QID 150009) may reflect a lower number than the combination of links and forms requested during the crawl.

IMPACT:

Some links that lead to different areas of the site's functionality may have been missed.

SOLUTION:

Increase the maximum number of links in order to ensure broader coverage of the Web application. It is important to note that increasing the number of links crawled can dramatically increase the time required to test the Web application.

RESULT:

Maximum request count reached: 300

Links Rejected By Crawl Scope or Exclusion List

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150020
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-02-07 16:48:28.0

THREAT:

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

IMPACT:

Links listed here were neither crawled or tested by the Web application scanning engine.

SOLUTION:

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

RESULT:

Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

External links discovered:
<https://www.facebook.com/wingpath>
<https://www.americanexpress.com/>
<https://www.se.com/>
<https://twitter.com/WingpathUK>
<http://www.paessler.com/tools/mibimporter>
<http://www.paypal.com/>

http://modbus.control.com/
http://www.modbus.org/
http://www.mastercard.com/
http://www.emersonprocess.com/

IP based excluded links:
Links rejected during the test phase not reported due to volume of links.

Web Server Versionport 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 86000
Category: Web server
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2021-12-20 13:32:52.0

THREAT:
A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.
IMPACT:
N/A
SOLUTION:
N/A
RESULT:
Apache/2.4.41 (Ubuntu)

Links Crawledport 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 150009
Category: Web Application
CVE ID: -

Vendor Reference: -
Bugtraq ID: -
Last Update: 2020-07-27 21:11:30.0

THREAT:

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

- NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
 - All the forms reported in QID 150152 (Forms Crawled)
 - All the forms in QID 150115 (Authentication Form Found)
 - Certain requests from QID 150172 (Requests Crawled)

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Duration of crawl phase (seconds): 3.00
Number of links: 2
(This number excludes form requests and links re-requested during authentication.)

<https://basil.wingpath.co.uk/>
<https://basil.wingpath.co.uk/manual>


Scan Diagnostics

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 150021
Category: Web Application
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2009-01-16 18:02:19.0

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page <https://wingpath.co.uk/> fetched. Status code:200, Content-Type:text/html, load time:90 milliseconds.

Ineffective Session Protection. no tests enabled.

Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)

[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase

CMSDetection: 1 vulnsigs tests, completed 38 requests, 4 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.

HSTS Analysis no tests enabled.

Maximum request count reached: 300

Collected 511 links overall in 0 hours 0 minutes duration.

Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)

BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 312) + files:(0 x 313) + directories:(9 x 27) + paths:(0 x 340) = total (243)

Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 340 inputs)

WS Directory Path manipulation: 9 vulnsigs tests, completed 243 requests, 3 seconds. Completed 243 requests of 243 estimated requests (100%). All tests completed.

WSEnumeration no tests enabled.

Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (70 tests, 20 inputs)

Batch #1 URI parameter manipulation (no auth): 70 vulnsigs tests, completed 1400 requests, 9 seconds. Completed 1400 requests of 1400 estimated requests (100%).

All tests completed.

Blind SQL manipulation - have 20 URI parameters,0 form fields - no tests enabled.

Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (16 tests, 20 inputs)

Batch #1 URI parameter time-based tests (no auth): 16 vulnsigs tests, completed 320 requests, 3 seconds. Completed 320 requests of 320 estimated requests (100%).

All tests completed.

Batch #2 URI parameter manipulation (no auth): estimated time < 1 minute (70 tests, 20 inputs)

Batch #2 URI parameter manipulation (no auth): 70 vulnsigs tests, completed 1400 requests, 12 seconds. Completed 1400 requests of 1400 estimated requests (100%).

All tests completed.

Batch #2 URI parameter time-based tests (no auth): estimated time < 1 minute (16 tests, 20 inputs)

Batch #2 URI parameter time-based tests (no auth): 16 vulnsigs tests, completed 320 requests, 3 seconds. Completed 320 requests of 320 estimated requests (100%).

All tests completed.

Batch #3 URI parameter manipulation (no auth): estimated time < 1 minute (70 tests, 17 inputs)

Batch #3 URI parameter manipulation (no auth): 70 vulnsigs tests, completed 1257 requests, 7 seconds. Completed 1257 requests of 1190 estimated requests

(105.63%). All tests completed.

Blind SQL manipulation - have 17 URI parameters,0 form fields - no tests enabled.

Batch #3 URI parameter time-based tests (no auth): estimated time < 1 minute (16 tests, 17 inputs)

Batch #3 URI parameter time-based tests (no auth): 16 vulnsigs tests, completed 272 requests, 2 seconds. Completed 272 requests of 272 estimated requests (100%).

All tests completed.

Batch #4 WebCgiOob: estimated time < 10 minutes (135 tests, 1 inputs)

Batch #4 WebCgiOob: 135 vulnsigs tests, completed 3060 requests, 43 seconds. Completed 3060 requests of 53720 estimated requests (5.6962%). All tests completed.

XXE tests no tests enabled.

Arbitrary File Upload no tests enabled.

Arbitrary File Upload On Status OK no tests enabled.

HTTP call manipulation no tests enabled.

SSL Downgrade. no tests enabled.

Open Redirect no tests enabled.

CSRF no tests enabled.

Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 319 inputs)

Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 319 estimated requests (0%). All tests completed.

Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 1 inputs)

Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 5184 requests, 34 seconds. Completed 5184 requests of 5148 estimated requests (100.699%). XSS optimization removed 8294 links. All tests completed.

Batch #4 Header manipulation: estimated time < 10 minutes (47 tests, 286 inputs)

Batch #4 Header manipulation: 47 vulnsigs tests, completed 18144 requests, 118 seconds. Completed 18144 requests of 37180 estimated requests (48.8004%). XSS optimization removed 8294 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 150 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 150 requests, 1 seconds. Completed 150 requests of 150 estimated requests (100%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

htpoxxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 312) + files:(0 x 313) + directories:(4 x 27) + paths:(11 x 340) = total (3848)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 340 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 3109 requests, 31 seconds. Completed 3109 requests of 3848 estimated requests (80.7952%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 312) + files:(4 x 313) + directories:(94 x 27) + paths:(5 x 340) = total (5490)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 340 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 4787 requests, 53 seconds. Completed 4787 requests of 5490 estimated requests (87.1949%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 1 hour (576 tests, 1 inputs)

Batch #5 WebCgiGeneric: 576 vulnsigs tests, completed 31443 requests, 407 seconds. Completed 31443 requests of 271660 estimated requests (11.5744%). All tests completed.

Duration of Crawl Time: 25.00 (seconds)

Duration of Test Phase: 726.00 (seconds)

Total Scan Time: 751.00 (seconds)

Total requests made: 71720

Average server response time: 0.06 seconds

Average browser load time: 0.06 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found

Default Web Page

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	12230
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-03-16 03:30:26.0

THREAT:

The Result section displays the default Web page for the Web server.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

GET / HTTP/1.1

Host: wingpath.co.uk

Connection: Keep-Alive

```
<!DOCTYPE html>
<html>
<head>
<title>Wingpath Software Development</title>
<link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" />
<link rel="icon" href="/favicon.ico" type="image/x-icon" />
<link rel="stylesheet" href="/wingpath.css" />
<meta charset=utf-8 />
<meta name="no-email-collection"
content="http://www.unspam.com/noemailcollection" />
<meta name="viewport" content="initial-scale=1" />
<meta property="og:title" content="Wingpath Software Development" />
<meta name="twitter:title" content="Wingpath Software Development" />
<meta name="twitter:site" content="@WingpathUK" />
<meta property="og:type" content="website" />
<meta property="fb:app_id" content="616894918895094" />
<script src="/js/jquery.min.js"></script>
<script src="/js/jquery-migrate.min.js"></script>
<meta name="description" content="Modbus products and custom software development in Java and C/C++ for Linux" />
<meta property="og:description" content="Modbus products and custom software development in Java and C/C++ for Linux" />
<meta name="twitter:description" content="Modbus products and custom software development in Java and C/C++ for Linux" />
<link rel="canonical" href="https://wingpath.co.uk/" />
<meta property="og:url" content="https://wingpath.co.uk/" />
<meta property="og:image" content="https://wingpath.co.uk/images/media.png" />
<meta name="twitter:card" content="summary_large_image" />
<meta name="twitter:image" content="https://wingpath.co.uk/images/media.png" />
</head>
<body>
<div id="page" >
<header>
<a href=".">

</a>
<div class="social_links"><a target=_blank rel=noopener class=social_link
href="https://www.facebook.com/wingpath"></a><a target=_blank rel=noopener class=social_link
href="https://twitter.com/WingpathUK"></a></div> </header>
```

```
<div id="main">
<div id="leftcolumn">
<div id="sidebar">
<nav>
<div>&nbsp;<a class="link" href="products.php" title="Software products">Products</a></div>
<div>&nbsp;<a class="link" href="custom_software.php" title="Custom software development">Custom&nbsp;&nbsp;software</a></div>
<div>&nbsp;<a class="link" href="help.php" title="Ordering information">Help</a></div>
<div>&nbsp;<a class="link" href="contact.php" title="How to contact us">Company&nbsp;&nbsp;details</a></div>

<div class="sidebarspacer">
</div>

<div>&nbsp;<a class="link" href="modbus/modbus_protocol.php" title="Modbus protocol information">Modbus&nbsp;&nbsp;protocol</a></div>
<div>&nbsp;<a class="link" href="modbus/modbus.php" title="Software for the Modbus protocol">Modbus&nbsp;&nbsp;software</a></div>

<div class="sidebarspacer">
</div>

<div>&nbsp;<a class="link" href="modbus/modsnmp.php" title="ModSnmp - Modbus-SNMP converter">ModSnmp</a></div>
<div>&nbsp;<a class="link" href="modbus/modmultisim.php" title="ModMultiSim - Programmable simulator for multiple Modbus slaves">ModMultiSim</a></div>
<div>&nbsp;<a class="link" href="modbus/modsak.php" title="Modsak - Versatile Modbus diagnostic tool">Modsak</a></div>
<div>&nbsp;<a class="link" href="modbus/modslavesim.php" title="ModSlaveSim - Programmable Modbus slave simulator">ModSlaveSim</a></div>
<div>&nbsp;<a class="link" href="modbus/modmaster.php" title="ModMaster - Diagnostic Modbus master">ModMaster</a></div>
<div>&nbsp;<a class="link" href="modbus/modtest.php" title="ModTest - Automated Modbus tester">ModTest</a></div>

<div class="sidebarspacer">
</div>

<div>&nbsp;<a class="link" href="register.php" title="Request or transfer a registration key">Registration</a></div>
<a class="link" href="hpterm.php"></a></nav>
</div>
</div>
<div id="maincolumn1"><div id="maincontent">
<h2>Wingpath Software</h2>

<p>Wingpath supplies
<a class="link" href="custom_software.php">custom software</a> and
<a class="link" href="products.php">Modbus software products</a>.
</p>

<p>In our professional Modbus product range we have a number of Modbus
test and configuration tools.
These help software developers, system integrators and field service engineers
to develop and maintain systems that use the Modbus protocol
and its many extensions.
The tools have evolved over many years in response to our own and
our clients&apos; needs when implementing and testing
industrial networks and software using Modbus.
</p>

<p><a class="link" href="modbus/modsak.php" title="Modsak - Versatile Modbus diagnostic tool">Modsak</a> is an all-purpose
Modbus test tool designed to act as a Modbus
slave, a Modbus master, or a bridge between master and slave.
</p>

<p>Like Modsak, <a class="link" href="modbus/modmultisim.php" title="ModMultiSim - Programmable simulator for multiple Modbus slaves">ModMultiSim</a> simulates
```

a Modbus slave but additionally allows highly realistic simulations of multiple slaves in their environment. If you simply want to simulate a single slave, try out [ModSlaveSim](modbus/modslavesim.php "ModSlaveSim - Programmable Modbus slave simulator").

If you are testing slave devices only, [ModMaster](modbus/modmaster.php "ModMaster - Diagnostic Modbus master") simulates a Modbus master.

All these tools have troubleshooting guides. In an area that has become overly complex through extensions and diverse interpretations from many device manufacturers, the troubleshooting guides provide invaluable help and reminders of what can go wrong.

We often provide enhancements as updates that are freely available to download after purchase.

Copyright 2003-2024 Wingpath Ltd

GET / HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 16 May 2024 11:00:34 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT
ETag: "2aa6-5f040bdba30ce"
Accept-Ranges: bytes
Content-Length: 10918
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
Modified from the Debian original for Ubuntu

Last updated: 2016-11-16

See: <https://launchpad.net/bugs/1288690>

-->

<head>

<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

<title>Apache2 Ubuntu Default Page: It works</title>

<style type="text/css" media="screen">

* {

margin: 0px 0px 0px 0px;

padding: 0px 0px 0px 0px;

}

body, html {

padding: 3px 3px 3px 3px;

background-color: #D8DBE2;

font-family: Verdana, sans-serif;

font-size: 11pt;

text-align: center;

}

div.main_page {

position: relative;

display: table;

width: 800px;

margin-bottom: 3px;

margin-left: auto;

margin-right: auto;

padding: 0px 0px 0px 0px;

border-width: 2px;

border-color: #212738;

border-style: solid;

background-color: #FFFFFF;

text-align: center;

}

div.page_header {

height: 99px;

width: 100%;

background-color: #F5F6F7;

}

div.page_header span {

margin: 15px 0px 0px 50px;

font-size: 180%;

font-weight: bold;

}


```
div.page_header img {  
margin: 3px 0px 0px 40px;
```

```
  
border: 0px 0px 0px;  
}
```

```
div.table_of_contents {  
clear: left;
```

```
  
min-width: 200px;
```

```
  
margin: 3px 3px 3px 3px;
```

```
  
background-color: #FFFFFF;
```

```
  
text-align: left;  
}
```

```
div.table_of_contents_item {  
clear: left;
```

```
  
width: 100%;
```

```
  
margin: 4px 0px 0px 0px;
```

```
  
background-color: #FFFFFF;
```

```
  
color: #000000;  
text-align: left;  
}
```

```
div.table_of_contents_item a {  
margin: 6px 0px 0px 6px;  
}
```

```
div.content_section {  
margin: 3px 3px 3px 3px;
```

```
  
background-color: #FFFFFF;
```

```
  
text-align: left;  
}
```

```
div.content_section_text {  
padding: 4px 8px 4px 8px;
```

```
  
color: #000000;  
font-size: 100%;  
}
```

```
div.content_section_text pre {  
margin: 8px 0px 8px 0px;  
padding: 8px 8px 8px 8px;
```

```
  
border-width: 1px;  
border-style: dotted;
```

border-color: #000000;

background-color: #F5F6F7;

font-style: italic;
}

div.content_section_text p {
margin-bottom: 6px;
}

div.content_section_text ul, div.content_section_text li {
padding: 4px 8px 4px 16px;
}

div.section_header {
padding: 3px 6px 3px 6px;

background-color: #8E9CB2;

color: #FFFFFF;
font-weight: bold;
font-size: 112%;
text-align: center;
}

div.section_header_red {
background-color: #CD214F;
}

div.section_header_grey {
background-color: #9F9386;
}

.floating_element {
position: relative;
float: left;
}

div.table_of_contents_item a,
div.content_section_text a {
text-decoration: none;
font-weight: bold;
}

div.table_of_contents_item a:link,
div.table_of_contents_item a:visited,
div.table_of_contents_item a:active {
color: #000000;
}

div.table_of_contents_item a:hover {
background-color: #000000;

color: #FFFFFF;
}

```
div.content_section_text a:link,
div.content_section_text a:visited,
div.content_section_text a:active {
background-color: #DCDFE6;

color: #000000;
}

div.content_section_text a:hover {
background-color: #000000;

color: #DCDFE6;
}

div.validator {
}
</style>
</head>
<body>
<div class="main_page">
<div class="page_header floating_element">

<span class="floating_element">
Apache2 Ubuntu Default Page
</span>
</div>
<!-- <div class="table_of_contents floating_element">
<div class="section_header section_header_grey">
TABLE OF CONTENTS
</div>
<div class="table_of_contents_item floating_element">
<a href="#about">About</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#changes">Changes</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#scope">Scope</a>
</div>
<div class="table_of_contents_item floating_element">
<a href="#files">Config files</a>
</div>
</div>
-->
<div class="content_section floating_element">

<div class="section_header section_header_red">
<div id="about"></div>
It works!
</div>
<div class="content_section_text">
<p>
This is the default welcome page used to test the correct
operation of the Apache2 server after installation on Ubuntu systems.
```

It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived.

If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance.

If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in** `/usr/share/doc/apache2/README.Debian.gz`. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the [manual](/manual) if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
| `-- ports.conf
|-- mods-enabled
| |-- *.load
| `-- *.conf
|-- conf-enabled
| `-- *.conf
|-- sites-enabled
| `-- *.conf
```

`apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

`ports.conf` is always included from the

main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.

Configuration files in the <tt>mods-enabled/</tt>, <tt>conf-enabled/</tt> and <tt>sites-enabled/</tt> directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.

They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers

<tt>

a2enmod,

a2dismod,

</tt>

<tt>

a2ensite,

a2dissite,

</tt>

and

<tt>

a2enconf,

a2disconf

</tt>. See their respective man pages for detailed information.

The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with <tt>/etc/init.d/apache2</tt> or <tt>apache2ctl</tt>. Calling <tt>/usr/bin/apache2</tt> directly will not work with the default configuration.

</div>

<div class="section_header">

<div id="docroot"></div>

Document Roots

</div>

<div class="content_section_text">

<p>

By default, Ubuntu does not allow access through the web browser to any file apart of those located in <tt>/var/www/</tt>, public_html directories (when enabled) and <tt>/usr/share/</tt> (for web applications). If your site is using a web document root located elsewhere (such as in <tt>/srv/</tt>) you may need to whitelist your document root directory in <tt>/etc/apache2/apache2.conf</tt>.

</p>

```
<p>
The default Ubuntu document root is <tt>/var/www/html</tt>. You
can make your own virtual hosts under /var/www. This is different
to previous releases which provides better security out of the box.
</p>
</div>
```

```
<div class="section_header">
<div id="bugs"></div>
Reporting Problems
</div>
<div class="content_section_text">
<p>
Please use the <tt>ubuntu-bug</tt> tool to report bugs in the
Apache2 package with Ubuntu. However, check <a
href="https://bugs.launchpad.net/ubuntu/+source/apache2"
rel="nofollow">existing bug reports</a> before reporting a new bug.
</p>
<p>
Please report bugs specific to modules (such as PHP and others)
to respective packages, not to the web server itself.
</p>
</div>
```

```
</div>
</div>
<div class="validator">
</div>
</body>
</html>
```

TLS Secure Renegotiation Extension Support Information

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	42350
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2016-03-21 16:40:23.0

THREAT:
Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
TLS Secure Renegotiation Extension Status: supported.


Web Server Supports HTTP Request Pipelining

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 86565

Category: Web server

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2005-02-23 00:25:38.0

THREAT:
Version 1.1 of the HTTP protocol supports URL-Request Pipelining. This means that instead of using the "Keep-Alive" method to keep the TCP connection alive over multiple requests, the protocol allows multiple HTTP URL requests to be made in the same TCP packet. Any Web server which is HTTP 1.1 compliant should then process all the URLs requested in the single TCP packet and respond as usual.

The target Web server was found to support this functionality of the HTTP 1.1 protocol.

IMPACT:
Support for URL-Request Pipelining has interesting consequences. For example, as explained in [this paper by Daniel Roelker](#), it can be used for evading detection by Intrusion Detection Systems. Also, it can be used in HTTP Response-Splitting style attacks.

SOLUTION:
N/A

RESULT:
GET / HTTP/1.1
Host:185.132.38.51:443

GET /Q_Evasive/ HTTP/1.1
Host:185.132.38.51:443

IP ID Values Randomness

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	82046
Category:	TCP/IP
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2006-07-27 21:45:19.0

THREAT:
The values for the identification (ID) field in IP headers in IP packets from the host are analyzed to determine how random they are. The changes between subsequent ID values for either the network byte ordering or the host byte ordering, whichever is smaller, are displayed in the RESULT section along with the duration taken to send the probes. When incremental values are used, as is the case for TCP/IP implementation in many operating systems, these changes reflect the network load of the host at the time this test was conducted.

Please note that for reliability reasons only the network traffic from open TCP ports is analyzed.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
IP ID changes observed (network order) for port 22: 0
Duration: 32 milli seconds

Scan Diagnosticsport 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150021
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2009-01-16 18:02:19.0

THREAT:

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

IMPACT:

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

SOLUTION:

No action is required.

RESULT:

Target web application page <https://basil.wingpath.co.uk/> fetched. Status code:200, Content-Type:text/html, load time:86 milliseconds.

Ineffective Session Protection. no tests enabled.

Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)

[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase

CMSDetection: 1 vulnsigs tests, completed 38 requests, 1 seconds. Completed 38 requests of 38 estimated requests (100%). All tests completed.

HSTS Analysis no tests enabled.

Collected 2 links overall in 0 hours 0 minutes duration.

Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)

BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 1) + directories:(9 x 2) + paths:(0 x 3) = total (18)

Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 3 inputs)

WS Directory Path manipulation: 9 vulnsigs tests, completed 18 requests, 0 seconds. Completed 18 requests of 18 estimated requests (100%). All tests completed.

WSEnumeration no tests enabled.

Batch #4 WebCgiOob: estimated time < 1 minute (135 tests, 1 inputs)

Batch #4 WebCgiOob: 135 vulnsigs tests, completed 27 requests, 0 seconds. Completed 27 requests of 474 estimated requests (5.6962%). All tests completed.

XXE tests no tests enabled.

Arbitrary File Upload no tests enabled.

Arbitrary File Upload On Status OK no tests enabled.

HTTP call manipulation no tests enabled.

SSL Downgrade. no tests enabled.

Open Redirect no tests enabled.

CSRF no tests enabled.

Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 2 inputs)

Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 2 estimated requests (0%). All tests completed.

Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 0 inputs)

Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 2 inputs)

Batch #4 Header manipulation: 47 vulnsigs tests, completed 126 requests, 1 seconds. Completed 126 requests of 260 estimated requests (48.4615%). XSS optimization removed 58 links. All tests completed.

Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 2 inputs)

Batch #4 shell shock detector: 1 vulnsigs tests, completed 2 requests, 0 seconds. Completed 2 requests of 2 estimated requests (100%). All tests completed.

Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)

Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

httpoxy no tests enabled.

Static Session ID no tests enabled.

Login Brute Force no tests enabled.

Login Brute Force manipulation estimated time: no tests enabled

Insecurely Served Credential Forms no tests enabled.

Cookies Without Consent no tests enabled.

Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)

Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 1) + directories:(4 x 2) + paths:(11 x 3) = total (41)

Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 3 inputs)

Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 40 requests, 0 seconds. Completed 40 requests of 41 estimated requests (97.561%). All tests completed.

Tomcat Vuln manipulation no tests enabled.

Time based path manipulation no tests enabled.

Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(4 x 1) + directories:(94 x 2) + paths:(5 x 3) = total (207)

Batch #5 Path manipulation: estimated time < 1 minute (103 tests, 3 inputs)

Batch #5 Path manipulation: 103 vulnsigs tests, completed 200 requests, 1 seconds. Completed 200 requests of 207 estimated requests (96.6184%). All tests completed.

WebCgiHrsTests: no test enabled

Batch #5 WebCgiGeneric: estimated time < 1 minute (576 tests, 1 inputs)

Batch #5 WebCgiGeneric: 576 vulnsigs tests, completed 510 requests, 3 seconds. Completed 510 requests of 2397 estimated requests (21.2766%). All tests completed.

Duration of Crawl Time: 3.00 (seconds)

Duration of Test Phase: 5.00 (seconds)

Total Scan Time: 8.00 (seconds)

Total requests made: 966

Average server response time: 0.03 seconds

Average browser load time: 0.03 seconds

Scan launched using pciwas_combined/pciwas_combined_new/pciwas_combined_v2 mode.

HTML form authentication unavailable, no WEBAPP entry found


Cookies Collected

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 

QID: 150028

Category: Web Application

CVE ID: -

Vendor Reference: -

Bugtraq ID: -

Last Update: 2020-02-19 18:46:27.0

THREAT:

The cookies listed in the Results section were set by the web application during the crawl phase.

IMPACT:

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

SOLUTION:

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

RESULT:

Total cookies: 1

uid=5066673620; expires=Fri May 16 10:12:16 2025; path=/; domain=wingpath.co.uk; max-age=31535980

Default Web Page (Follow HTTP Redirection)

port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	13910
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-11-05 13:13:22.0

THREAT:
The Result section displays the default Web page for the Web server following HTTP redirections.

IMPACT:
N/A

SOLUTION:
N/A

Patch:
Following are links for downloading patches to fix the vulnerabilities:

[nas-201911-01](#)

RESULT:
GET / HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

PhpMyAdmin Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	11954
Category:	CGI
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-05-13 03:31:37.0

THREAT:

phpMyAdmin is a free software tool written in PHP, intended to handle the administration of MySQL over the Web. phpMyAdmin supports a wide range of operations on MySQL and MariaDB.

QID Detection Logic (Unauthenticated):

The qid sends a GET request to "doc/html/index.html" and "Documentation.html" pages to retrieve the PhpMyAdmin version.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

PhpMyAdmin Detected on port: 443
GET /phpmyadmin/index.php HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

```
<!DOCTYPE HTML><html lang=en&apos; dir=ltr&apos;><head><meta charset=utf-8" /><meta name="referrer" content="no-referrer" /><meta name="robots" content="noindex,nofollow" /><meta http-equiv="X-UA-Compatible" content="IE=Edge" /><meta name="viewport" content="width=device-width, initial-scale=1.0"><style id="cfs-style">html{display: none;}</style><link rel="icon" href="favicon.ico" type="image/x-icon" /><link rel="shortcut icon" href="favicon.ico" type="image/x-icon" /><link rel="stylesheet" type="text/css" href="/themes/pmahomme/jquery/jquery-ui.css" /><link rel="stylesheet" type="text/css" href="js/vendor/codemirror/lib/codemirror.css?v=4.9.5deb2" /><link rel="stylesheet" type="text/css" href="js/vendor/codemirror/addon/hint/show-hint.css?v=4.9.5deb2" /><link rel="stylesheet" type="text/css" href="js/vendor/codemirror/addon/lint/lint.css?v=4.9.5deb2" /><link rel="stylesheet" type="text/css" href="phpmyadmin.css.php?nocache=4755212520ltr&server=1" /><link rel="stylesheet" type="text/css" href="/themes/pmahomme/css/printview.css?v=4.9.5deb2" media="print" id="printcss"/><title>phpMyAdmin</title><script data-cfasync=false" type="text/javascript" src="js/vendor/jquery/jquery.min.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/vendor/jquery/jquery-migrate.js?v=4.9.5deb2"></script><script data-cfasync=&apos;false&apos; type=&apos;text/javascript&apos; src=&apos;js/whitelist.php?v=4.9.5deb2&lang=en&apos;></script><script data-cfasync=false" type="text/javascript" src="js/vendor/sprintf.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/ajax.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/keyhandler.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/vendor/jquery/jquery-ui.min.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/vendor/js.cookie.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/vendor/jquery/jquery.mousewheel.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/vendor/jquery/jquery.event.drag-2.2.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/vendor/jquery/jquery.validate.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/vendor/jquery/jquery-ui-timepicker-addon.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/vendor/jquery/jquery.ba-hashchange-1.3.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/vendor/jquery/jquery.debounce-1.0.5.js?v=4.9.5deb2"></script><script data-cfasync=false" type="text/javascript" src="js/menu-resizer.js?v=4.9.5deb2"></script>
```

```
<script data-cfasync="false" type="text/javascript" src="js/cross_framing_protection.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/rte.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/vendor/tracekit.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/error_report.js?v=4.9.5deb2"></script>
<script data-cfasync=&apos;false&apos; type=&apos;text/javascript&apos; src=&apos;js/messages.php?l=en&amp;v=4.9.5deb2&amp;lang=en&apos;></script>
<script data-cfasync="false" type="text/javascript" src="js/config.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/doclinks.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/functions.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/navigation.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/indexes.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/common.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/page_settings.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/shortcuts_handler.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/vendor/codemirror/lib/codemirror.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/vendor/codemirror/mode/sql/sql.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/vendor/codemirror/addon/runmode/runmode.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/vendor/codemirror/addon/hint/show-hint.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/vendor/codemirror/addon/hint/sql-hint.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/vendor/codemirror/addon/lint/lint.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/codemirror/addon/lint/sql-lint.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript" src="js/console.js?v=4.9.5deb2"></script>
<script data-cfasync="false" type="text/javascript">/*! [CDATA[
PMA_commonParams.setAll({common_query:"?lang=en",opendb_url:"db_structure.php",lang:"en",server:"1",table:"",db:"",token:"212e242355693f61657c21673b654e50",
text_dir:"ltr",show_databases_navigation_as_tree:true,pma_text_default_tab:"Browse",pma_text_left_default_tab:"Structure",pma_text_left_default_tab2:false,LimitChars:"
50",pftext:"",confirm:true,LoginCookieValidity:"1440",session_gc_maxlifetime:"1440",logged_in:false,is_https:true,rootPath:"/phpmyadmin/",arg_separator:"&",
PMA_VERSION:"4.9.5deb2",auth_type:"cookie",user:"root"});
ConsoleEnterExecutes=false
AJAX.scriptHandler.add("vendor/jquery/jquery.min.js",0).add("vendor/jquery/jquery-migrate.js",0).add("whitelist.php",1).add("vendor/sprintf.js",1).add("ajax.js",0).add
("keyhandler.js",1).add("vendor/jquery/jquery-ui.min.js",0).add("vendor/js.cookie.js",1).add("vendor/jquery/jquery.mousewheel.js",0).add("vendor/jquery/jquery.event.drag-
2.2.js",0).add("vendor/jquery/jquery.validate.js",0).add("vendor/jquery/jquery-ui-timepicker-addon.js",0).add("vendor/jquery/jquery.ba-hashchange-1.3.js",0).add("vendor
/jquery/jquery.debounce-1.0.5.js",0).add("menu-resizer.js",1).add("cross_framing_protection.js",0).add("rte.js",1).add("vendor/tracekit.js",1).add("error_report.js",1).add
("messages.php",0).add("config.js",1).add("doclinks.js",1).add("functions.js",1).add("navigation.js",1).add("indexes.js",1).add("common.js",1).add("page_settings.js",1).add
("shortcuts_handler.js",1).add("vendor/codemirror/lib/codemirror.js",0).add("vendor/codemirror/mode/sql/sql.js",0).add("vendor/codemirror/addon/runmode/runmode.js",0).
add("vendor/codemirror/addon/hint/show-hint.js",0).add("vendor/codemirror/addon/hint/sql-hint.js",0).add("vendor/codemirror/addon/lint/lint.js",0).add("codemirror/addon
/lint/sql-lint.js",0).add("console.js",1);
$(function() {AJAX.fireOnload("whitelist.php");AJAX.fireOnload("vendor/sprintf.js");AJAX.fireOnload("keyhandler.js");AJAX.fireOnload("vendor/js.cookie.js");AJAX.
fireOnload("menu-resizer.js");AJAX.fireOnload("rte.js");AJAX.fireOnload("vendor/tracekit.js");AJAX.fireOnload("error_report.js");AJAX.fireOnload("config.js");AJAX.
fireOnload("doclinks.js");AJAX.fireOnload("functions.js");AJAX.fireOnload("navigation.js");AJAX.fireOnload("indexes.js");AJAX.fireOnload("common.js");AJAX.fireOnload
("page_settings.js");AJAX.fireOnload("shortcuts_handler.js");AJAX.fireOnload("console.js");});
// ]]></script><noscript><style>html{display:block}</style></noscript></head><body id=&apos;loginform&apos;><div id="pma_header"></div><div id="page_content"
><div class="container">
<a href="/url.php?url=https%3A%2F%2Fwww.phpmyadmin.net%2F" target="_blank" rel="noopener noreferrer" class="logo">

</a>
<h1>Welcome to <bdo dir="ltr" lang="en">phpMyAdmin</bdo></h1>

<noscript>
<div class="error"> Javascript must be enabled past this point!</div>
</noscript>

<div class="hide" id="js-https-mismatch">
<div class="error"> There is mismatch between HTTPS indicated on the server and client. This can lead
to non working phpMyAdmin or a security risk. Please fix your server configuration to indicate HTTPS properly.</div>
</div>
<div class=&apos;hide js-show&apos;> <form method="get" action="index.php" class="disableAjax">
<input type="hidden" name="db" value="" /><input type="hidden" name="table" value="" /><input type="hidden" name="lang" value="en" /><input type="hidden" name="
```

```
token" value="212e242355693f61657c21673b654e50" />

<fieldset>
<legend lang="en" dir="ltr">Language</legend>

<select name="lang" class="autosubmit" lang="en" dir="ltr" id="sel-lang">

<option value="sq">
Shqip - Albanian
</option>
<option value="ar">
&#1575;&#1604;&#1593;&#1585;&#1576;&#1610;&#1577; - Arabic
</option>
<option value="hy">
- Armenian
</option>
<option value="az">
Az&#601;rbaycanca - Azerbaijani
</option>
<option value="bn">
- Bangla
</option>
<option value="be">
&#1041;&#1077;&#1083;&#1072;&#1088;&#1091;&#1089;&#1082;&#1072;&#1103; - Belarusian
</option>
<option value="pt_br">
Portugu&ecirc;s - Brazilian Portuguese
</option>
<option value="bg">
&#1041;&#1098;&#1083;&#1075;&#1072;&#1088;&#1089;&#1082;&#1080; - Bulgarian
</option>
<option value="ca">
Catal&agrave; - Catalan
</option>
<option value="zh_cn">
&#20013;&#25991; - Chinese simplified
</option>
<option value="zh_tw">
&#20013;&#25991; - Chinese traditional
</option>
<option value="cs">
etina - Czech
</option>
<option value="da">
Dansk - Danish
</option>
<option value="nl">
Nederlands - Dutch
</option>
<option value="en" selected="selected">
English
</option>
<option value="en_gb">
English (United Kingdom)
</option>
<option value="et">
```

Eesti - Estonian
</option>
<option value="fi">
Suomi - Finnish
</option>
<option value="fr">
Français - French
</option>
<option value="gl">
Galego - Galician
</option>
<option value="de">
Deutsch - German
</option>
<option value="el">
Ελληνικά - Greek
</option>
<option value="he">
עברית - Hebrew
</option>
<option value="hu">
Magyar - Hungarian
</option>
<option value="id">
Bahasa Indonesia - Indonesian
</option>
<option value="ia">
Interlingua
</option>
<option value="it">
Italiano - Italian
</option>
<option value="ja">
日本語 - Japanese
</option>
<option value="kk">
- Kazakh
</option>
<option value="ko">
한국어 - Korean
</option>
<option value="lt">
Lietuvių - Lithuanian
</option>
<option value="nb">
Norsk - Norwegian
</option>
<option value="pl">
Polski - Polish
</option>
<option value="pt">
Português - Portuguese
</option>
<option value="ro">
Română - Romanian
</option>

```
<option value="ru">
&#1056;&#1091;&#1089;&#1089;&#1082;&#1080;&#1081; - Russian
</option>
<option value="sr@latin">
Srpski - Serbian (latin)
</option>
<option value="si">
&#3523;&#3538;&#3458;&#3524;&#3517; - Sinhala
</option>
<option value="sk">
Sloven&#269;ina - Slovak
</option>
<option value="sl">
Sloven&scaron;&#269;ina - Slovenian
</option>
<option value="es">
Espa&ntilde;ol - Spanish
</option>
<option value="sv">
Svenska - Swedish
</option>
<option value="th">
&#3616;&#3634;&#3625;&#3634;&#3652;&#3607;&#3618; - Thai
</option>
<option value="tr">
T&uuml;r&ccedil;e - Turkish
</option>
<option value="uk">
&#1059;&#1082;&#1088;&#1072;&#1111;&#1085;&#1089;&#1100;&#1082;&#1072; - Ukrainian
</option>
<option value="vi">
Ting Vit - Vietnamese
</option>

</select>

</fieldset>

</form>
</div>
<br />
<!-- Login form -->
<form method="post" id="login_form" action="index.php" name="login_form" class="disableAjax login hide js-show">
<fieldset>
<legend><input type="hidden" name="set_session" value="3aileid5cgekki911sq7nujdht" />Log in<a href="/.doc/html/index.html" target="documentation"></a></legend><div class="item">
<label for="input_username">Username:</label>
<input type="text" name="pma_username" id="input_username" value="" size="24" class="textfield"/>
</div>
<div class="item">
<label for="input_password">Password:</label>
<input type="password" name="pma_password" id="input_password" value="" size="24" class="textfield" />
</div> <input type="hidden" name="server" value="1" /></fieldset><fieldset class="tblFooters"><input value="Go" type="submit" id="input_go" /><input type="hidden"
name="target" value="index.php" /><input type="hidden" name="lang" value="en" /><input type="hidden" name="token" value="212e242355693f61657c21673b654e50"
/></fieldset>
</form></div>
```


<div id="pma_footer"></div></div></body></html>-CR-

External Links Discovered

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150010
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-02-19 18:30:56.0

THREAT:

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Number of links: 43

<https://www.facebook.com/wingpath>

<https://www.americanexpress.com/>

<https://www.se.com/>

<https://twitter.com/WingpathUK>

<http://www.paessler.com/tools/mibimporter>

<http://www.paypal.com/>

<http://modbus.control.com/>

<http://www.modbus.org/>

<http://www.mastercard.com/>

<http://www.emersonprocess.com/>

<http://www.emersonprocess.com/daniel/default.htm>

[http://www05.abb.com/global/scot/scot267.nsf/veritydisplay/e2cc269455559c3d85256cd300640eff/\\$file/2100741AIAA.pdf](http://www05.abb.com/global/scot/scot267.nsf/veritydisplay/e2cc269455559c3d85256cd300640eff/$file/2100741AIAA.pdf)

<http://www.java.com/>

<http://www.snmp4j.org/>

http://www.snmp4j.org/LICENSE-2_0.txt

<http://modbus.org/>

http://modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf

http://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

http://modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

http://modbus.org/docs/Modbus_over_serial_line_V1_02.pdf

http://modbus.org/docs/PI_MBUS_300.pdf

<http://modbus.org/specs.php>

<http://www.visa.com/>

http://www2.emersonprocess.com/siteadmincenter/PM%20Daniel%20Documents/3-9000-545.pdf
http://tools.ietf.org/html/rfc1157
http://tools.ietf.org/html/rfc2578
http://tools.ietf.org/html/rfc2579
http://tools.ietf.org/html/rfc2580
http://tools.ietf.org/html/rfc3410
http://tools.ietf.org/html/rfc3411
http://tools.ietf.org/html/rfc3412
http://tools.ietf.org/html/rfc3413
http://tools.ietf.org/html/rfc3414
http://tools.ietf.org/html/rfc3415
http://tools.ietf.org/html/rfc3416
http://tools.ietf.org/html/rfc3417
http://tools.ietf.org/html/rfc3418
http://tools.ietf.org/html/rfc3584
http://tools.ietf.org/html/rfc4181
http://www.schneider-electric.com/
http://logging.apache.org/log4j/1.2/
http://www.ietf.org/
http://www.apache.org/licenses/LICENSE-2.0.html

HTTP Public-Key-Pins Security Header Not Detected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	48002
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-07-12 15:16:39.0

THREAT:
HTTP Public Key Pinning (HPKP) is a security feature that tells a web client to associate a specific cryptographic public key with a certain web server to decrease the risk of MITM attacks with forged certificates.

QID Detection Logic:
This QID detects the absence of the Public-Key-Pins HTTP header by transmitting a GET request.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP Public-Key-Pins Header missing on port 443.
GET / HTTP/1.1

Host: wingpath.co.uk
Connection: Keep-Alive

SSL Session Caching Information

port 25 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1
QID: 38291
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2020-03-19 22:48:23.0

THREAT:
SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

IMPACT:
SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

SOLUTION:
N/A

RESULT:
TLSv1 session caching is enabled on the target.
TLSv1.1 session caching is enabled on the target.
TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is enabled on the target.

Apache HTTP Server Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1

QID:	45391
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2022-09-26 18:24:45.0

THREAT:

The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

Apache HTTP Server was detected on the target.

QID Detection Logic (Authenticated):

Operating System: Linux

The detection looks for Apache HTTP Server installation path using ps command. The version is extracted from the Apache HTTP Server's binary.

Operating System: Windows

This QID checks Windows registry to see if Apache HTTP Server is installed. If found, it displays the installed version.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Apache web server detected on port 80 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 282

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
```

Apache web server detected on port 443 -

Date: Thu, 16 May 2024 10:12:08 GMT

Server: Apache/2.4.41 (Ubuntu)

Content-Length: 309

Connection: close

Content-Type: text/html; charset=iso-8859-1

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
```

```
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at coppermist.co.uk Port 443</address>
</body></html>
```

List of Web Directories

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	86672
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:57.0

THREAT:
Based largely on the HTTP reply code, the following directories are most likely present on the host.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

- Directory Source**
- /phpmyadmin/ brute force
 - /js/ brute force
 - /icons/ brute force
 - /javascript/ brute force
 - /js/jquery/ brute force
 - /icons/ web page
 - /phpmyadmin/ web page
 - /phpmyadmin/js/ web page
 - /phpmyadmin/js/vendor/ web page
 - /phpmyadmin/js/vendor/jquery/ web page
 - /phpmyadmin/js/vendor/codemirror/ web page
 - /phpmyadmin/js/vendor/codemirror/lib/ web page
 - /phpmyadmin/js/vendor/codemirror/addon/ web page
 - /phpmyadmin/js/vendor/codemirror/addon/hint/ web page
 - /phpmyadmin/js/vendor/codemirror/addon/lint/ web page
 - /phpmyadmin/_static/ web page

HTTP Response Method and Header Information Collected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
HTTP header and method information collected on port 443.

GET / HTTP/1.1
Host: wingpath.co.uk
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Thu, 16 May 2024 10:40:14 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 6287
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=utf-8

List of Web Directories Requiring Authentication

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	86671
Category:	Web server
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2004-09-10 23:40:09.0

THREAT:
The service has identified a list of Web directories which require authentication to access.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Directories Requiring Authentication
/admin/

Scan Activity per Port

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	45426
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-06-24 12:42:21.0

THREAT:
Scan activity per port is an estimate of the amount of internal process time the scanner engine spent scanning a particular TCP or UDP port. This information can be useful to determine the reason for long scan times. The individual time values represent internal process time, not elapsed time, and can be longer than the total scan time because of internal parallelism. High values are often caused by slowly responding services or services on which requests time out.

IMPACT:
N/A

SOLUTION:

N/A

RESULT:

Protocol Port
Time

TCP 22 0:11:01

TCP 25 0:04:31

TCP 80 5:42:30

TCP 443 8:22:48

Web Server Versionport 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:1
QID:86000
Category:Web server
CVE ID:-
Vendor Reference:-
Bugtraq ID:-
Last Update:2021-12-20 13:32:52.0

THREAT:

A web server is server software, or hardware dedicated to running this software, that can satisfy client requests on the World Wide Web.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Apache/2.4.41 (Ubuntu)

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	45004
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2013-08-15 21:12:37.0

THREAT:
The information shown in the Result section was returned by the network infrastructure responsible for routing traffic from our cloud platform to the target network (where the scanner appliance is located).

This information was returned from: 1) the WHOIS service, or 2) the infrastructure provided by the closest gateway server to our cloud platform. If your ISP is routing traffic, your ISP's gateway server returned this information.

IMPACT:
This information can be used by malicious users to gather more information about the network infrastructure that may help in launching attacks against it.

SOLUTION:
N/A

RESULT:
The network handle is: RIPE-185
Network description:
RIPE Network Coordination Centre

HTTP Response Method and Header Information Collected

port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	48118
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-20 12:24:23.0

THREAT:
This QID prints the information, in the form of a text record, that a web server sends back to a client's browser in response to receiving a single HTTP GET request.

QID Detection Logic:
This QID returns the HTTP response method and header information returned by a web server.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

HTTP header and method information collected on port 443.

GET / HTTP/1.1

Host: basil.wingpath.co.uk

Connection: Keep-Alive

HTTP/1.1 200 OK

Date: Thu, 16 May 2024 11:00:34 GMT

Server: Apache/2.4.41 (Ubuntu)

Last-Modified: Tue, 20 Dec 2022 11:28:55 GMT

ETag: "2aa6-5f040bdba30ce"

Accept-Ranges: bytes

Content-Length: 10918

Vary: Accept-Encoding

Keep-Alive: timeout=5, max=96

Connection: Keep-Alive

Content-Type: text/html

Secure Sockets Layer (SSL) Certificate Transparency Information

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38718
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2021-06-08 21:07:04.0

THREAT:

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

IMPACT:

N/A

SOLUTION:

N/A

RESULT:

Source Validated Name URL ID Time


Certificate #0 CN=wingpath.co.uk
Certificate no (unknown) (unknown) 3f174b4fd7224758941d651c84be0d12ed90377f1f856aebc1bf2885ecf8646e Thu 01 Jan 1970 12:00:00 AM GMT
Certificate no (unknown) (unknown) eecdd064d5db1acec55cb79db4cd13a23287467cbcecddec351485946711fb59b Thu 01 Jan 1970 12:00:00 AM GMT
Certificate #0 CN=coppermist.co.uk
Certificate no (unknown) (unknown) 1998107109f0d6522e3080d29e3f64bb836e28ccf90f528eedfce4a3f16b4ca Thu 01 Jan 1970 12:00:00 AM GMT
Certificate no (unknown) (unknown) 3f174b4fd7224758941d651c84be0d12ed90377f1f856aebc1bf2885ecf8646e Thu 01 Jan 1970 12:00:00 AM GMT

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity: 1 
QID: 38597
Category: General remote services
CVE ID: -
Vendor Reference: -
Bugtraq ID: -
Last Update: 2021-07-12 23:14:58.0

THREAT:
SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

my version	target version
0304	0303
0399	0303
0400	0303
0499	0303

Links Crawled port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	150009
Category:	Web Application
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2020-07-27 21:11:30.0

THREAT:
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

- NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
 - All the forms reported in QID 150152 (Forms Crawled)
 - All the forms in QID 150115 (Authentication Form Found)
 - Certain requests from QID 150172 (Requests Crawled)

IMPACT:
N/A

SOLUTION:
N/A

RESULT:
Duration of crawl phase (seconds): 3.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

<http://basil.wingpath.co.uk/>

SSL Server Information Retrieval

port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1 <div><div></div><div></div><div></div><div></div><div></div></div>
QID:	38116
Category:	General remote services
CVE ID:	-
Vendor Reference:	-

Bugtraq ID: -
Last Update: 2016-05-24 21:02:48.0

THREAT:

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

IMPACT:
N/A

SOLUTION:
N/A

RESULT:

CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE

SSLv2 PROTOCOL IS DISABLED

SSLv3 PROTOCOL IS DISABLED

TLSv1 PROTOCOL IS DISABLED

TLSv1.1 PROTOCOL IS DISABLED

TLSv1.2 PROTOCOL IS ENABLED

TLSv1.2 COMPRESSION METHOD None

ECDHE-ECDSA-AES128-GCM-SHA256 ECDH ECDSA AEAD AESGCM(128) MEDIUM

ECDHE-ECDSA-AES256-GCM-SHA384 ECDH ECDSA AEAD AESGCM(256) HIGH

ECDHE-ECDSA-CHACHA20-POLY1305 ECDH ECDSA AEAD CHACHA20/POLY1305(256) HIGH

TLSv1.3 PROTOCOL IS ENABLED

TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(128) MEDIUM

TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH

TLS13-CHACHA20-POLY1305-SHA256 N/A N/A AEAD CHACHA20/POLY1305(256) HIGH

Appendices

Hosts Scanned
185.132.38.51

Hosts Not Alive

Option Profile

Scan	
Scanned TCP Ports:	Full
Scanned UDP Ports:	Standard Scan
Scan Dead Hosts:	Off
Load Balancer Detection:	Off
Password Brute Forcing	Standard
Vulnerability Detection	Complete
Windows Authentication:	Disabled
SSH Authentication:	Disabled
Oracle Authentication:	Disabled
SNMP Authentication:	Disabled
Perform 3-way Handshake:	Off

Advanced	
Hosts Discovery:	TCP Standard Scan, UDP Standard Scan, ICMP On
Ignore RST packets:	Off
Ignore firewall-generated SYN-ACK packets:	Off
Do not send ACK or SYN-ACK packets during host discovery:	Off

Report Legend

Payment Card Industry (PCI) Status

An overall PCI compliance status of PASSED indicates that all hosts in the report passed the PCI compliance standards. A PCI compliance status of PASSED for a single host/IP indicates that no vulnerabilities or potential vulnerabilities, as defined by the PCI DSS compliance standards set by the PCI Council, were detected on the host.

An overall PCI compliance status of FAILED indicates that at least one host in the report failed to meet the PCI compliance standards. A PCI compliance status of FAILED for a single host/IP indicates that at least one vulnerability or potential vulnerability, as defined by the PCI DSS compliance standards set by the PCI Council, was detected on the host.

Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
<div><div></div><div></div><div></div><div></div><div></div></div>	1 Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
<div><div></div><div></div><div></div><div></div><div></div></div>	2 Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.

<div><div></div><div></div><div></div><div></div><div></div></div>	3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
<div><div></div><div></div><div></div><div></div><div></div></div>	4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
<div><div></div><div></div><div></div><div></div><div></div></div>	5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
<div>LOW</div>	Low	A vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
<div>MED</div>	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
<div>HIGH</div>	High	A vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description	
<div><div></div><div></div><div></div><div></div><div></div></div>	1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
<div><div></div><div></div><div></div><div></div><div></div></div>	2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
<div><div></div><div></div><div></div><div></div><div></div></div>	3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
<div><div></div><div></div><div></div><div></div><div></div></div>	4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
<div><div></div><div></div><div></div><div></div><div></div></div>	5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilites at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Severity	Level	Description
<div>LOW</div>	Low	A potential vulnerability with a CVSS base score of 0.0 through 3.9. These vulnerabilities are not required to be fixed to pass PCI compliance.
<div>MED</div>	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
<div>HIGH</div>	High	A potential vulnerability with a CVSS base score of 7.0 through 10.0. These vulnerabilities must be fixed to pass PCI compliance.

Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
<div><div></div><div></div><div></div><div></div><div></div></div>	1 Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
<div><div></div><div></div><div></div><div></div><div></div></div>	2 Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
<div><div></div><div></div><div></div><div></div><div></div></div>	3 Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.