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		FAIL

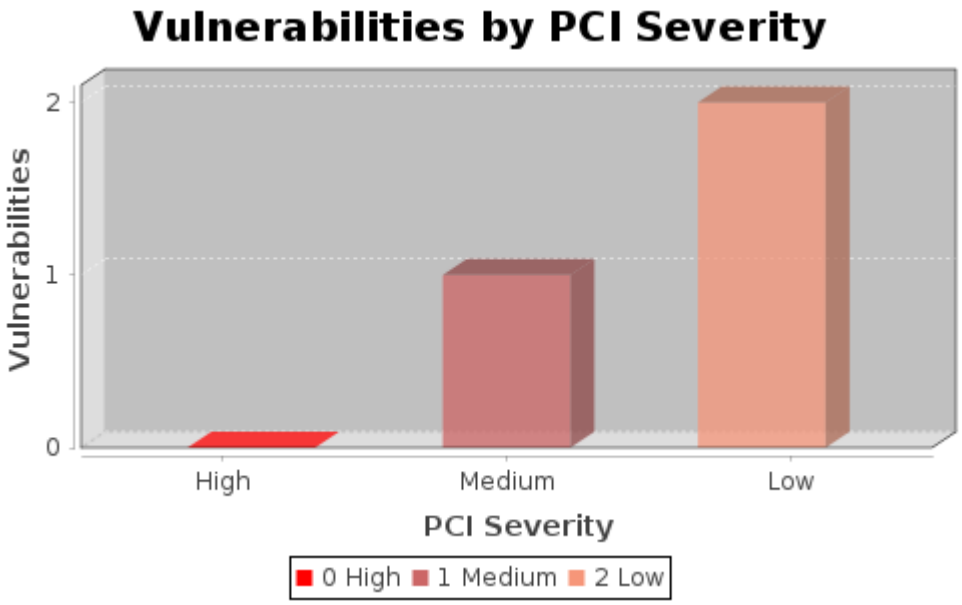
Report Summary	
Company:	WWW.WINGPATH.CO.UK
Hosts in account	1
Hosts scanned	1
Hosts active	1
Scan date	May 26, 2024
Report date	May 26, 2024

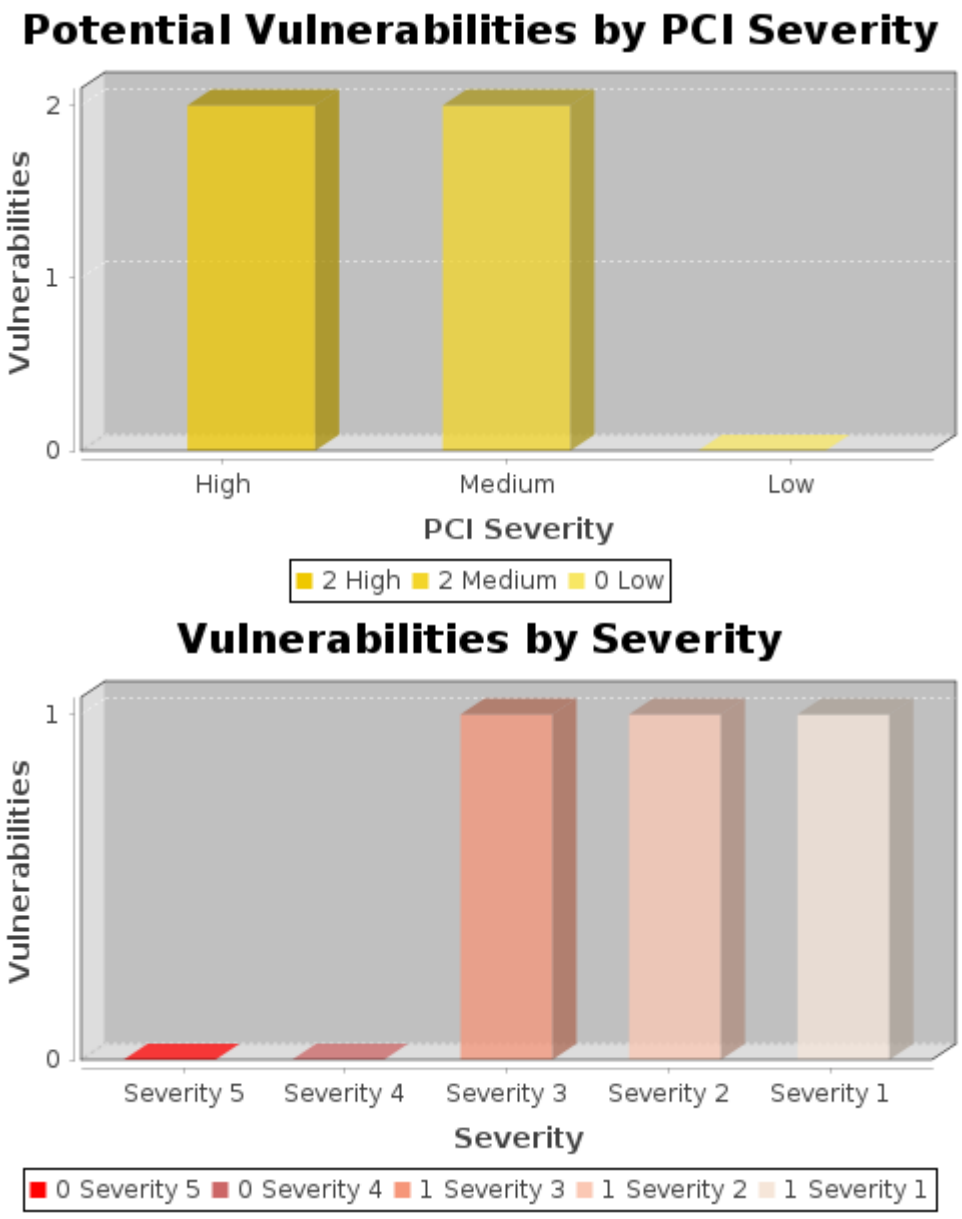
Summary of Vulnerabilities

Vulnerabilities total:	56	Security risk:	4

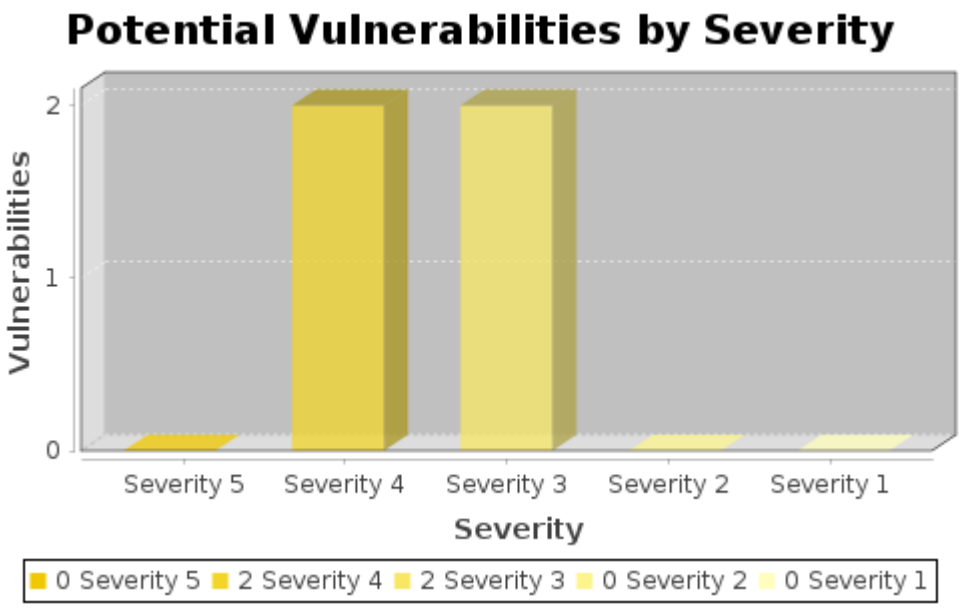
by Severity				
Severity	**Confirmed**	**Potential**	**Information gathered**	**Total**
5	0	0	0	0
4	0	2	0	2
3	1	2	1	4
2	1	0	4	5
1	1	0	44	45
Total	3	4	49	56

by PCI Severity			
PCI Severity	**Confirmed**	**Potential**	**Total**
High	0	2	2
Medium	1	2	3
Low	2	0	2
Total	3	4	7




Potential Vulnerabilities by PCI Severity
Vulnerabilities
2
1
0
High
Medium
Low
PCI Severity
2 High
2 Medium
0 Low

Vulnerabilities by Severity
Vulnerabilities
1
0
Severity 5
Severity 4
Severity 3
Severity 2
Severity 1
Severity
0 Severity 5
0 Severity 4
1 Severity 3
1 Severity 2
1 Severity 1


Potential Vulnerabilities by Severity
Vulnerabilities
2
1
0
Severity 5
Severity 4
Severity 3
Severity 2
Severity 1
Severity
0 Severity 5
2 Severity 4
2 Severity 3
0 Severity 2
0 Severity 1

Detailed Results

185.132.38.51 (basil.wingpath.co.uk,) Linux 2.6

Vulnerabilities total:	56	Security risk:	4

Vulnerabilities (3)

TCP Sequence Number Approximation Based Denial of Service

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:	**4.3** E:F/RL:T/RC:C
Severity:	**3**
QID:	82054
Category:	TCP/IP
CVE ID:	CVE-2004-0230
Vendor Reference:	-
Bugtraq ID:	10183
Last Update:	2024-02-29 00:00:01.0

THREAT:

TCP provides stateful communications between hosts on a network. TCP sessions are established by a three-way handshake and use random 32-bit sequence and acknowledgement numbers to ensure the validity of traffic. A vulnerability was reported that may permit TCP sequence numbers to be more easily approximated by remote attackers. This issue affects products released by multiple vendors.

The cause of the vulnerability is that affected implementations will accept TCP sequence numbers within a certain range, known as the acknowledgement range, of the expected sequence number for a packet in the session. This is determined by the TCP window size, which is negotiated during the three-way handshake for the session. Larger TCP window sizes may be set to allow for more throughput, but the larger the TCP window size, the more probable it is to guess a TCP sequence number that falls within an acceptable range. It was initially thought that guessing an acceptable sequence number was relatively difficult for most implementations given random distribution, making this type of attack impractical. However, some implementations may make it easier to successfully approximate an acceptable TCP sequence number, making these attacks possible with a number of protocols and implementations.

This is further compounded by the fact that some implementations may support the use of the TCP Window Scale Option, as described in RFC 1323, to extend the TCP window size to a maximum value of 1 billion.

This vulnerability will permit a remote attacker to inject a SYN or RST packet into the session, causing it to be reset and effectively allowing for denial of service attacks. An attacker would exploit this issue by sending a packet to a receiving implementation with an approximated sequence number and a forged source IP address and TCP port.

There are a few factors that may present viable target implementations, such as those which depend on long-lived TCP connections, those that have known or easily guessed IP address endpoints and those implementations with easily guessed TCP source ports. It has been noted that Border Gateway Protocol (BGP) is reported to be particularly vulnerable to this type of attack, due to the use of long-lived TCP sessions and the possibility that some implementations may use the TCP Window Scale Option. As a result, this issue is likely to affect a number of routing platforms.

Another factor to consider is the relative difficulty of injecting packets into TCP sessions, as a number of receiving implementations will reassemble packets in order, dropping any duplicates. This may make some implementations more resistant to attacks than others.

It should be noted that while a number of vendors have confirmed this issue in various products, investigations are ongoing and it is likely that many other vendors and products will turn out to be vulnerable as the issue is investigated further.

IMPACT:
Successful exploitation of this issue could lead to denial of service attacks on the TCP based services of target hosts.

SOLUTION:
Please first check the results section below for the port number on which this vulnerability was detected. If that port number is known to be used for port-forwarding, then it is the backend host that is really vulnerable.

Various implementations and products including Check Point, Cisco, Cray Inc, Hitachi, Internet Initiative Japan, Inc (IIJ), Juniper Networks, NEC and Yamaha are currently undergoing review. Contact the vendors to obtain more information about affected products and fixes. NISCC Advisory 236929 - Vulnerability Issues in TCP details the vendor patch status as of the time of the advisory, and identifies resolutions and workarounds.

Refer to US-CERT Vulnerability Note VU#415294 and OSVDB Article 4030 to obtain a list of vendors affected by this issue and a note on resolutions (if any) provided by the vendor.

For Microsoft: Refer to MS05-019 and MS06-064 for further details.

For SGI IRIX: Refer to SGI Security Advisory 20040905-01-P

For SCO UnixWare 7.1.3 and 7.1.1: Refer to SCO Security Advisory SCOSA-2005.14

For Solaris (Sun Microsystems): The vendor has acknowledged the vulnerability; however a patch is not available. Refer to Sun Microsystems, Inc. Information for VU#415294 to obtain additional details. Also, refer to TA04-111A for detailed mitigating strategies against these attacks.

For NetBSD: Refer to NetBSD-SA2004-006

For Cisco: Refer to cisco-sa-20040420-tcp-ios.shtml.

For IBM : Refer to IBM-tcp-sequence-number-cve-2004-0230.

For Red Hat Linux: There is no fix available : Refer to .

Workaround:
The following BGP-specific workaround information has been provided.

For BGP implementations that support it, the TCP MD5 Signature Option should be enabled. Passwords that the MD5 checksum is applied to should be set to strong values and changed on a regular basis.

Secure BGP configuration instructions have been provided for Cisco and Juniper at these locations:
Secure Cisco IOS BGP Template
JUNOS Secure BGP Template

RESULT:
Tested on port 80 with an injected SYN/RST offset by 16 bytes.

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**
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

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 be 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): 11:56:51 GMT

Potential Vulnerabilities (4)

Apache HTTP Server Prior to 2.4.59 Multiple Security Vulnerabilities — port 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**
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/1.1 301 Moved Permanently
Date: Sun, 26 May 2024 12:00:06 GMT
Server: Apache/2.4.58 (Ubuntu)
Location: https://wingpath.co.uk/
Content-Length: 317
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>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at basil.wingpath.co.uk Port 80</add

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**
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/1.1 301 Moved Permanently
Date: Sun, 26 May 2024 12:00:11 GMT
Server: Apache/2.4.58 (Ubuntu)

Location: https://wingpath.co.uk/
Content-Length: 318
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>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at basil.wingpath.co.uk Port 443</ad

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**
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: Sun, 26 May 2024 12:00:00 GMT
Server: Apache/2.4.58 (Ubuntu)
Location: https://wingpath.co.uk/
Content-Length: 317
Connection: close
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>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>

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: Sun, 26 May 2024 12:00:00 GMT
Server: Apache/2.4.58 (Ubuntu)
Content-Length: 313
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>
Your browser sent a request that this server could not understand.

<hr>
<address>Apache/2.4.58 (Ubuntu) Server at basil.wingpath.co.uk Port 443</address>
</body></html>

Information Gathered (49)

Remote Access or Management Service Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**3**
QID:	42017
Category:	General remote services
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-05-20 12:30:20.0

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.

Host Uptime Based on TCP TimeStamp Option

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
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 35 days, 8 hours, and 23 minutes.
The TCP timestamps from the host are in units of 1 milliseconds.

Web Server HTTP Protocol Versions — port 443 / 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 443 port.GET / HTTP/1.1

Operating System Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**2**
QID:	45017
Category:	Information gathering
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2024-05-20 12:30:20.0

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
Linux 2.6 TCP/IP Fingerprint U6991:
22

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

IP ID Values Randomness

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
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 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Duration: 30 milli seconds

Referrer-Policy HTTP Security Header Not Detected port 443 / 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 443 port.
GET / HTTP/1.1
Host: basil.wingpath.co.uk
Connection: Keep-Alive

DNS Host Name

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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

Scan Diagnostics port 80 / 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 http://basil.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.
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.

Potential LDAP Login Bypass no tests enabled.
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 (581 tests, 1 inputs)
Batch #5 WebCgiGeneric: 581 vulnsigs tests, completed 200 requests, 1 seconds. Completed 200 requests of 808 estimated requests (24.7525%). All tests completed.
Duration of Crawl Time: 4.00 (seconds)
Duration of Test Phase: 2.00 (seconds)
Total Scan Time: 6.00 (seconds)

Total requests made: 436
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

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: basil.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>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at basil.wingpath.co.uk Port 443</address>
</body></html>

TLS Secure Renegotiation Extension Support Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**

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.

HTTP Response Method and Header Information Collected — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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/1.1 301 Moved Permanently
Date: Sun, 26 May 2024 12:00:49 GMT
Server: Apache/2.4.58 (Ubuntu)
Location: https://wingpath.co.uk/
Content-Length: 317
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

Degree of Randomness of TCP Initial Sequence Numbers

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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 1167937299 with a standard deviation of 613639320. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5085 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is: hard.

Links Crawled port 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): 2.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

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

Default Web Page — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
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>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at basil.wingpath.co.uk Port 443</address>
</body></html>

Scan Activity per Port

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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	0:06:35
TCP 80	2:06:11
TCP 443	2:08:03

SSL Certificate - Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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 03:b3:7c:15:33:f2:7d:90:0d:e0:b9:0f:b3:90:7d:f3:8f:15
(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 22 12:45:10 2024 GMT
(0)Valid Till Aug 20 12:45:09 2024 GMT
(0)Public Key Algorithm id-ecPublicKey
(0)EC Public Key
(0) Public-Key: (256 bit)
(0) pub:
(0) 04:ff:93:5d:c5:32:3a:fb:5d:9e:54:64:e8:a1:6c:

(0) 1d:c0:06:ed:02:ee:6d:fa:6f:16:09:ea:d6:52:c5:
(0) b3:82:c4:14:bf:ff:c1:82:07:cd:1d:a4:db:3e:d6:
(0) 98:6a:53:ac:0d:d9:57:50:d5:4a:b5:31:99:1a:59:
(0) 8d:35:99:e5:6e
(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 52:8E:07:AD:16:04:B0:DC:0C:F3:4B:6B:16:93:46:0C:32:4E:2D: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:basil.wingpath.co.uk, DNS:coppermist.co.uk, 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 : 76:FF:88:3F:0A:B6:FB:95:51:C2:61:CC:F5:87:BA:34:
(0) B4:A4:CD:BB:29:DC:68:42:0A:9F:E6:67:4C:5A:3A:74
(0) Timestamp : May 22 13:45:10.776 2024 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:45:02:21:00:83:F3:47:63:B9:49:E1:28:20:8E:A9:
(0) 80:5C:CB:F8:B0:11:BD:D4:89:56:B4:FB:82:05:20:80:
(0) EB:A0:A7:63:9C:02:20:1C:56:08:C9:C5:F8:0D:7B:DA:
(0) FE:46:BC:73:D0:FC:D0:02:7D:BD:9A:38:CC:C0:CB:27:
(0) 0D:9E:92:89:CE:F0:DF
(0) Signed Certificate Timestamp:
(0) Version : v1 (0x0)
(0) Log ID : 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB:
(0) 1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73
(0) Timestamp : May 22 13:45:10.703 2024 GMT
(0) Extensions: none
(0) Signature : ecdsa-with-SHA256
(0) 30:45:02:21:00:A7:8A:AF:A2:19:73:A9:08:CB:99:8E:
(0) 6A:B0:7C:E9:B3:3A:BA:31:6C:33:23:CC:3F:9F:6F:A2:
(0) D3:93:9C:A2:B3:02:20:5C:06:B2:27:4D:05:03:EB:03:
(0) 9F:0E:51:3E:FC:72:DA:CB:55:B6:46:3D:9A:24:2C:81:
(0) A0:95:54:BF:C9:FD:3D
(0)Signature (256 octets)
(0) 62:db:5f:2f:33:87:45:79:27:61:e8:36:8b:7c:f7:6b
(0) 8c:36:8f:35:a3:7d:70:f6:86:42:c8:24:f6:94:eb:43
(0) d0:66:cf:07:4a:bc:fd:3d:a9:eb:89:04:6c:81:0c:e3
(0) 65:04:33:91:ca:1c:17:70:dc:f0:5f:b5:30:1f:10:3d
(0) fb:ab:71:4e:64:6d:7b:63:1e:e3:53:87:39:eb:32:73
(0) f6:a0:00:c8:f7:11:83:70:28:60:62:60:6c:98:e7:ad
(0) e7:7d:d6:36:c2:6e:af:60:95:e4:7a:cb:c1:36:d3:cd
(0) fa:1b:c0:9e:34:6d:53:5c:1d:4b:2e:aa:74:db:f3:7a
(0) 10:b7:01:7f:79:ba:25:dc:ff:5c:1c:82:d8:80:64:48
(0) c6:57:c3:69:be:be:14:50:ac:3e:16:5c:77:e6:f8:83
(0) 0e:ce:b3:07:b6:4a:72:47:4d:fc:e5:66:d0:e2:05:39
(0) 7f:69:16:08:a5:c7:6f:ff:df:ac:fe:0a:d3:dc:ff:2a

(0) 07:0e:47:fb:ba:6d:b5:5b:0b:18:f8:6f:6b:35:6f:1e
(0) cf:4c:33:32:e5:77:93:96:4e:07:6f:63:ec:30:31:c7
(0) 3b:eb:cb:2e:59:98:86:1b:73:bf:02:82:dd:80:ad:1a
(0) 08:0f:e0:79:a0:71:05:ba:d3:32:93:4a:88:ce:2a:f1
(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

Links Crawled port 80 / 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): 4.00
Number of links: 1
(This number excludes form requests and links re-requested during authentication.)

http://basil.wingpath.co.uk/

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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 DHE ffdhe2048 2048 yes 110 low
TLS13-AES-128-GCM-SHA256 DHE ffdhe3072 3072 yes 132 low
TLS13-AES-128-GCM-SHA256 DHE ffdhe4096 4096 yes 150 low
TLS13-AES-128-GCM-SHA256 DHE ffdhe6144 6144 yes 178 low
TLS13-AES-128-GCM-SHA256 DHE ffdhe8192 8192 yes 202 low
TLS13-AES-256-GCM-SHA384 DHE ffdhe2048 2048 yes 110 low
TLS13-AES-256-GCM-SHA384 DHE ffdhe3072 3072 yes 132 low
TLS13-AES-256-GCM-SHA384 DHE ffdhe4096 4096 yes 150 low
TLS13-AES-256-GCM-SHA384 DHE ffdhe6144 6144 yes 178 low
TLS13-AES-256-GCM-SHA384 DHE ffdhe8192 8192 yes 202 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe2048 2048 yes 110 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe3072 3072 yes 132 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe4096 4096 yes 150 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe6144 6144 yes 178 low
TLS13-CHACHA20-POLY1305-SHA256 DHE ffdhe8192 8192 yes 202 low
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

Links Rejected By Crawl Scope or Exclusion List — port 80 / 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://wingpath.co.uk/

IP based excluded links:
Links rejected during the test phase not reported due to volume of links.

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

SSL Server Information Retrieval — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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

Web Server Version — port 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/2.4.58 (Ubuntu)

Default Web Page — port 80 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
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>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>

Host Names Found

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
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

SSL Session Caching Information — port 443 / 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:
TLSv1.2 session caching is enabled on the target.
TLSv1.3 session caching is enabled on the target.

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://basil.wingpath.co.uk/ fetched. Status code:301, Content-Type:text/html, load time:85 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, 1 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.
Potential LDAP Login Bypass no tests enabled.
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 (581 tests, 1 inputs)
Batch #5 WebCgiGeneric: 581 vulnsigs tests, completed 200 requests, 1 seconds. Completed 200 requests of 808 estimated requests (24.7525%). All tests completed.
Duration of Crawl Time: 2.00 (seconds)
Duration of Test Phase: 3.00 (seconds)
Total Scan Time: 5.00 (seconds)

Total requests made: 436
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

ICMP Replies Received

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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 11:56:51
GMT

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/2.4.58 (Ubuntu)

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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

Firewall Detected

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
QID:	34011
Category:	Firewall
CVE ID:	-
Vendor Reference:	-
Bugtraq ID:	-
Last Update:	2019-04-22 02:37:57.0

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, 25, 53, 111, 135, 445, 1, 7.

Listed below are the ports filtered by the firewall.
No response has been received when any of these ports are probed.
1-21,23-79,81-442,444-6128,6130-65535

Secure Sockets Layer (SSL) Certificate Transparency Information — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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=coppermist.co.uk

Certificate no (unknown) (unknown) 76ff883f0ab6fb9551c261ccf587ba34b4a4cdbb29dc68420a9fe6674c5a3a74 Thu 01 Jan 1970 12:00:00 AM GMT

Certificate no (unknown) (unknown) 48b0e36bdaa647340fe56a02fa9d30eb1c5201cb56dd2c81d9bbbfab39d88473 Thu 01 Jan 1970 12:00:00 AM GMT

HTTP Response Method and Header Information Collected — port 443 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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/1.1 301 Moved Permanently
Date: Sun, 26 May 2024 12:09:24 GMT
Server: Apache/2.4.58 (Ubuntu)
Location: https://wingpath.co.uk/
Content-Length: 318
Keep-Alive: timeout=5, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

SSL Certificate will expire within next six months — port 443 / tcp over ssl

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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=coppermist.co.uk The certificate will expire within six months: Aug 20 12:45:09 2024 GMT

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: basil.wingpath.co.uk
Connection: Keep-Alive

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: 1
https://wingpath.co.uk/

Traceroute

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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
1 140.91.222.87 0.01ms ICMP
2 80.249.213.176 0.63ms ICMP
3 80.249.210.180 19.14ms ICMP
4 212.227.117.77 18.38ms ICMP
5 212.227.117.2 25.08ms ICMP
6 212.227.117.200 27.50ms ICMP
7 212.227.120.123 27.80ms ICMP
8 *.*.*.* 0.00ms Other 80
9 109.228.63.159 28.67ms ICMP
10 185.132.38.51 28.72ms ICMP

Internet Service Provider

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
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

SSH Banner — port 22 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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_9.6p1 Ubuntu-3ubuntu13

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: 1
https://wingpath.co.uk/

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: 2290 seconds

Start time: Sun, May 26 2024, 11:56:49 GMT

End time: Sun, May 26 2024, 12:34:59 GMT

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
80 www-http World Wide Web HTTP http
443 https http protocol over TLS/SSL http over ssl

Default Web Page (Follow HTTP Redirection) port 80 / tcp

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: basil.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>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>

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-Spliting 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

HTTP/1.1 301 Moved Permanently
Date: Sun, 26 May 2024 12:09:18 GMT
Server: Apache/2.4.58 (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>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at 185.132.38.51 Port 443</address>
</body></html>
HTTP/1.1 301 Moved Permanently
Date: Sun, 26 May 2024 12:09:18 GMT
Server: Apache/2.4.58 (Ubuntu)
Location: https://wingpath.co.uk/Q_Evasive/
Content-Length: 321
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>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at 185.132.38.51 Port 443</address>
</body></html>

SSH daemon information retrieving — port 22 / tcp

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	1
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 authentification 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 authentification 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 sntrup761x25519-sha512@openssh.com,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,ext-info-s,kex-strict-s-v00@openssh.com
Supported host key algorithms for SSH2 rsa-sha2-512,rsa-sha2-256,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

Target Network Information

PCI COMPLIANCE STATUS

PASS

VULNERABILITY DETAILS

Severity:	**1**
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

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://wingpath.co.uk/

IP based excluded links:
Links rejected during the test phase not reported due to volume of links.

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: Sun, 26 May 2024 12:00:00 GMT
Server: Apache/2.4.58 (Ubuntu)
Location: https://wingpath.co.uk/
Content-Length: 317
Connection: close
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>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at basil.wingpath.co.uk Port 80</address>
</body></html>
Apache web server detected on port 443 -
Date: Sun, 26 May 2024 12:00:00 GMT
Server: Apache/2.4.58 (Ubuntu)
Content-Length: 313
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>
Your browser sent a request that this server could not understand.

<hr>
<address>Apache/2.4.58 (Ubuntu) Server at basil.wingpath.co.uk Port 443</address>
</body></html>

Web Server Supports HTTP Request Pipelining — port 80 / tcp

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-Spliting 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/1.1 301 Moved Permanently
Date: Sun, 26 May 2024 12:09:18 GMT
Server: Apache/2.4.58 (Ubuntu)
Location: https://wingpath.co.uk/
Content-Length: 310
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>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at 185.132.38.51 Port 80</address>
</body></html>
HTTP/1.1 301 Moved Permanently
Date: Sun, 26 May 2024 12:09:18 GMT
Server: Apache/2.4.58 (Ubuntu)
Location: https://wingpath.co.uk/Q_Evasive/
Content-Length: 320
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>
The document has moved here.
<hr>
<address>Apache/2.4.58 (Ubuntu) Server at 185.132.38.51 Port 80</address>
</body></html>

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
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.
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.

	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.
	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.
	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
LOW	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.
MED	Medium	A vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	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
	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.
	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.
	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.
	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.
	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
LOW	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.
MED	Medium	A potential vulnerability with a CVSS base score of 4.0 through 6.9. These vulnerabilities must be fixed to pass PCI compliance.
HIGH	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
■□□□□	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.
■■□□□	2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
■■■□□	3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.