Server Configuration (/cpsess5613815762/scripts/command?PFILE=Server_Configuration)
Basic WebHost Manager® Setup (/cpsess5613815762/scripts/editsets)
Change Root Password (/cpsess5613815762/scripts/chrootpass)
Configure cPanel Analytics (/cpsess5613815762/scripts6/configure_cpanel_analytics)
Configure cPanel Cron Jobs (/cpsess5613815762/scripts/cronconfig)
Initial Quota Setup (/cpsess5613815762/scripts/dialog?dialog=quotas)
Server Profile (/cpsess5613815762/scripts7/server_profile)
Server Time (/cpsess5613815762/scripts/edittime)
Statistics Software Configuration (/cpsess5613815762/cgi/statmanager.cgi)
Terminal (/cpsess5613815762/scripts12/terminal)
Tweak Settings (/cpsess5613815762/scripts2/tweaksettings)
Update Preferences (/cpsess5613815762/scripts2/updateconf)
Support (/cpsess5613815762/scripts/command?PFILE=Support)
Create Support Ticket (/cpsess5613815762/scripts7/create_support_ticket)
Grant cPanel Support Access (/cpsess5613815762/scripts7/authorizesupport)
Support Center (/cpsess5613815762/scripts2/submitsupport)
Networking Setup

cPanel Security Advisor

Cpanel::Security::Advisor::Assessors::SSH 1.01 **Version:** 1.04

Important

Apache vhosts are not segmented or chroot()ed.

Enable “Jail Apache” in the “Tweak Settings (../../scripts2/tweaksettings?find=jailapache)” area, and change users to jailshell in the “Manage Shell Access (../../scripts2/manageshells)” area. Consider a more robust solution by using “CageFS on CloudLinux (https://go.cpanel.net/cloudlinux)”. Note that this may break the ability to access mailman via Apache.

Kernel does not support the prevention of symlink ownership attacks.

You do not appear to have any symlink protection enabled through a properly patched kernel on this server, which provides additional protections beyond those solutions employed in userland. Please review the documentation (https://go.cpanel.net/EA4Symlink) to learn how to apply this protection.

ClamAV is not installed.

Install ClamAV within "Manage Plugins (../../scripts2/manage_plugins)".

Trivially weak passwords are permitted.

Configure Password Strength requirements in the “Password Strength Configuration (../../scripts/minpwstrength)” area

Detected 17 processes that are running outdated executables: 18310 1833 1224 1969 1977 1965 1075 1818 1967 1971 1 17803 1372 32138 1976 18411 1974

Reboot the server (../../scripts/dialog?dialog=reboot) to ensure the system benefits from these updates.

SSH direct root logins are permitted.

Manually edit /etc/ssh/sshd_config and change PermitRootLogin to “without-password” or “no”, then restart SSH in the “Restart SSH (../../scripts/ressshd)” area

Verified