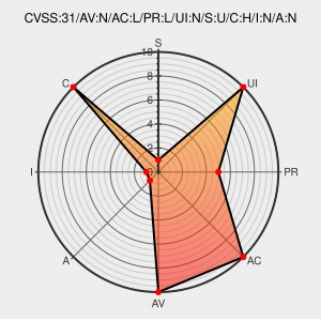
CVE-2019-14782

Published on: 12/17/2019 12:00:00 AM UTC

Last Modified on: 01/24/2023 06:57:00 PM UTC

CVE-2019-14782

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Centos Web Panel from Centos-webpanel contain the following vulnerability:

CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.856 through 0.9.8.864 allows an attacker to get a victim's session file name from the /tmp directory, and the victim's token value from /usr/local/cwpsrv/logs/access_log, then use them to make a request to extract the victim's password (for the OS and phpMyAdmin) via an attacker account.

CVE-2019-14782 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
ChangeLog for CentOS 7 | CentOS Web Panel	Release Notes, Vendor Advisory	MISC centos-webpanel.com/changelog-cwp7

	centos-webpanel.com text/html	
Control Web Panel 0.9.8.864 phpMyAdmin Password Disclosure ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/155676/Control-Web-Panel-0.9.8.864-phpMyAdmin-Password-Disclosure.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Centos-webpanel	Centos Web Panel	All	All	All	All
Application	Control-webpanel	Webpanel	All	All	All	All

cpe:2.3:a:centos-webpanel:centos_web_panel:*:*:*:*:*:*:*:*:

cpe:2.3:a:control-webpanel:webpanel:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→