Hive Pro

THREAT ADVISORY

CWP bugs cause RCE in Linux servers

TA2022019

Threat Level AMBER

Publish Date – Jan 26, 2022

Control Web Panel (CWP) has two vulnerabilities that affect approximately 200k servers that, when combined, could allow an attacker to gain unauthenticated remote code execution (RCE) as root on susceptible Linux servers.

The first is a file inclusion vulnerability (CVE-2021-45467), which lets an attacker to use a malicious API key to deliver a null byte powered file inclusion payload, and the second is a file write vulnerability (CVE-2021-45466), which when chained with the first one allows an attacker to write to a file using an API key.

An unauthenticated attacker can take advantage of these vulnerabilities by changing the include statement, which is used to insert script from one PHP file into another before the server runs it. The actual problem exists when two of the application's unauthenticated PHP pages, "/user/login.php" and "/user/index.php," fail to properly validate a path to a script file. A PoC of this exploit would be released by the researchers once most of the vulnerable Linux servers have been updated.

Both these vulnerabilities affect CWP Versions till 0.9.8.1120 and has been fixed in version 0.9.8.1122.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-45467	CWP Versions till 0.9.8.1120	cpe:2.3:a:centos-webpanel:centos_web_panel:*:*:*:*:*:*:*:*	Control Web Panel file inclusion vulnerability	CWE-98
CVE-2021-45466			Control Web Panel file write vulnerability	CWE-862

References

https://octagon.net/blog/2022/01/22/cve-2021-45467-cwp-centos-web-panel-preauth-rce/
https://www.reddit.com/r/netsec/comments/s9yb7s/cve202145467_cwp_centos_web_panel_preauth_rce/htyd9be/
https://threatpost.com/linux-servers-rce-critical-cwp-bugs/177906/
https://www.thesecmaster.com/how-to-fix-cve-2021-45467-a-remote-code-execution-vulnerability-in-control-web-panel/