Immediately patch CWP vulnerability that allows code execution as root on Linux servers

Security researchers have discovered two new vulnerabilities affecting Control Web Panel (CWP) software. Hackers could chain these two vulnerabilities to gain remote code execution (RCE) privileges as root on vulnerable Linux servers.

CWP, formerly known as CentOS Web Panel, is a free Linux control panel for managing dedicated web hosting servers and virtual private servers. The two vulnerabilities were discovered by Octagon Networks researcher Paulos Yibelo. They are tracked under the codes CVE-2021-45467 (file inclusion vulnerability) and CVE-2021-45466 (file write vulnerability) and can be chained to an RCE attack.

In short, when successfully exploiting these two vulnerabilities, hackers can bypass protections to gain access to restricted APIs without authentication.

This can be done by registering an API key via the include file vulnerability and creating a malicious authorized_keys file on the server using the file write vulnerability.

Although the vulnerability includes a patched file CVE-2021-45467, Octagon Network says it has found a way to bypass the patch and continue to exploit some of the servers. Security researchers at Octagon Network claim that when a sufficient number of Linux servers running CWP are patched, they will make their exploits (POCs) public.

According to the developers of CWP, their software supports the following operating systems: CentOS, Rocky Linux, Alma Linux and Oracle Linux.

While the CWP homepage claims that there are about 30,000 servers running CWP, news site BleepingComputer reports that nearly 80,000 servers running CWP are exposed to the Internet on BinaryEdge. More than 200,000 other CWP servers can be found on Shodan and Censys.