FORTINET

OUTBREAK ALERTS

CWP Control Web Panel Command Injection Vulnerability

A Linux control panel vulnerability exploited in the wild

https://control-webpanel.com/changelog#1669855527714-450fd335-6194

CVEs: CVE-2022-44877

A command injection vulnerability that allows remote attackers to easily exploit CWP (Control Web Panel) with a crafted HTTP request which can result in Remote Code Execution. According to Shodan, there are thousands of servers that could still be vulnerable to CVE-2022-44877. This vulnerability can be leveraged to perform ransomware attacks or exfiltration of data.

Background

Control Web Panel, formerly known as CentOS Web Panel, is a popular server administration tool for enterprise-based Linux systems. In the previous year, vulnerabilities (CVE-2021-45466 & CVE-2021-454667) related to CWP were released which may be used to exploit a preauth remote command execution.

Announced

Aug 25, 2022: CWP released security patches for CVE-2022-44877 at https://control-webpanel.com/changelog#1674073133745-94af1b53-c121

Latest Developments

Jan 17, 2023: CISA added CVE-2022-44877 to known exploited vulnerability (KEV) list at https://www.cisa.gov/known-exploited-vulnerabilities-catalog

FortiGuard Labs released an IPS signature and has observed attack attempts targeting the CWP vulnerability. FortiGuard Labs also recommends its customers to update their CWP to the latest version as soon as possible.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- **Delivery**

AV

Detects malware related to CWP Vulnerability (CVE-2022-44877)

FortiGate — DB 90.09765
FortiWeb — DB 90.09765
FortiClient — DB 90.09765
FortiSASE — DB 90.09765
FortiMail — DB 90.09765
FortiCASB — DB 90.09765
FortiCWP — DB 90.09765
FortiADC — DB 90.09765
FortiProxy — DB 90.09765

Vulnerability

Detects Linux systems running vulnerable CWP Control Web Panel (CVE-2022-44877)

FortiClient — DB 2.135

AV (Pre-filter)

Detects malware related to CWP Vulnerability (CVE-2022-44877)

FortiEDR — DB 90.09765
FortiSandbox — DB 90.09765
FortiNDR — DB 90.09765

- **Exploitation**

IPS

Blocks attack attempts related to CWP Vulnerability (CVE-2022-44877)

FortiGate — DB 22.479
FortiSASE — DB 22.479
FortiNDR — DB 22.479
FortiADC — DB 22.479
FortiProxy — DB 22.479

Web App Security

Blocks attack attempts related to CWP Vulnerability (CVE-2022-44877)

FortiWeb — DB 0.0034

Application Firewall

Blocks attack attempts related to CWP Vulnerability (CVE-2022-44877)

FortiClient — DB 22.479

- Installation
- C2
- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiClient — DB 1.005
FortiAnalyzer — DB 1.00084

IOC

FortiAnalyzer — DB 6.02444
FortiSIEM — DB 6.02444
FortiSOCaaS — DB 6.02444

Threat Hunting

FortiAnalyzer — v6.4+
FortiSIEM — v6.6+

Content Update

FortiSIEM — v6.6+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.

Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

Security Rating
FortiRecon: EASM
FortiDAST

Additional Resources

Security Week — https://www.securityweek.com/exploitation-control-web-panel-vulnerability-starts-after-poc-publication

The Hacker News — https://thehackernews.com/2023/01/alert-hackers-actively-exploiting.html

Bleeping Computer — https://www.bleepingcomputer.com/news/security/hackers-exploit-control-web-panel-flaw-to-open-reverse-shells/

Learn more about FortiGuard Outbreak Alerts

FORTINET