# OUTBREAK ALERTS 🗘



### **CWP Control Web Panel Command Injection** Vulnerability

#### A Linux control panel vulnerability exploited in the wild

https://control-webpanel.com/changelog#1669855527714-450fb335-6194 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#1674073133745-84af1b53-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.



O

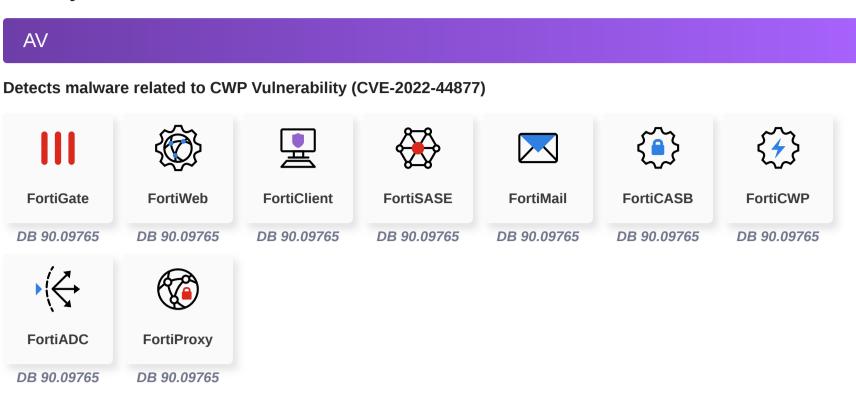
### PROTECT

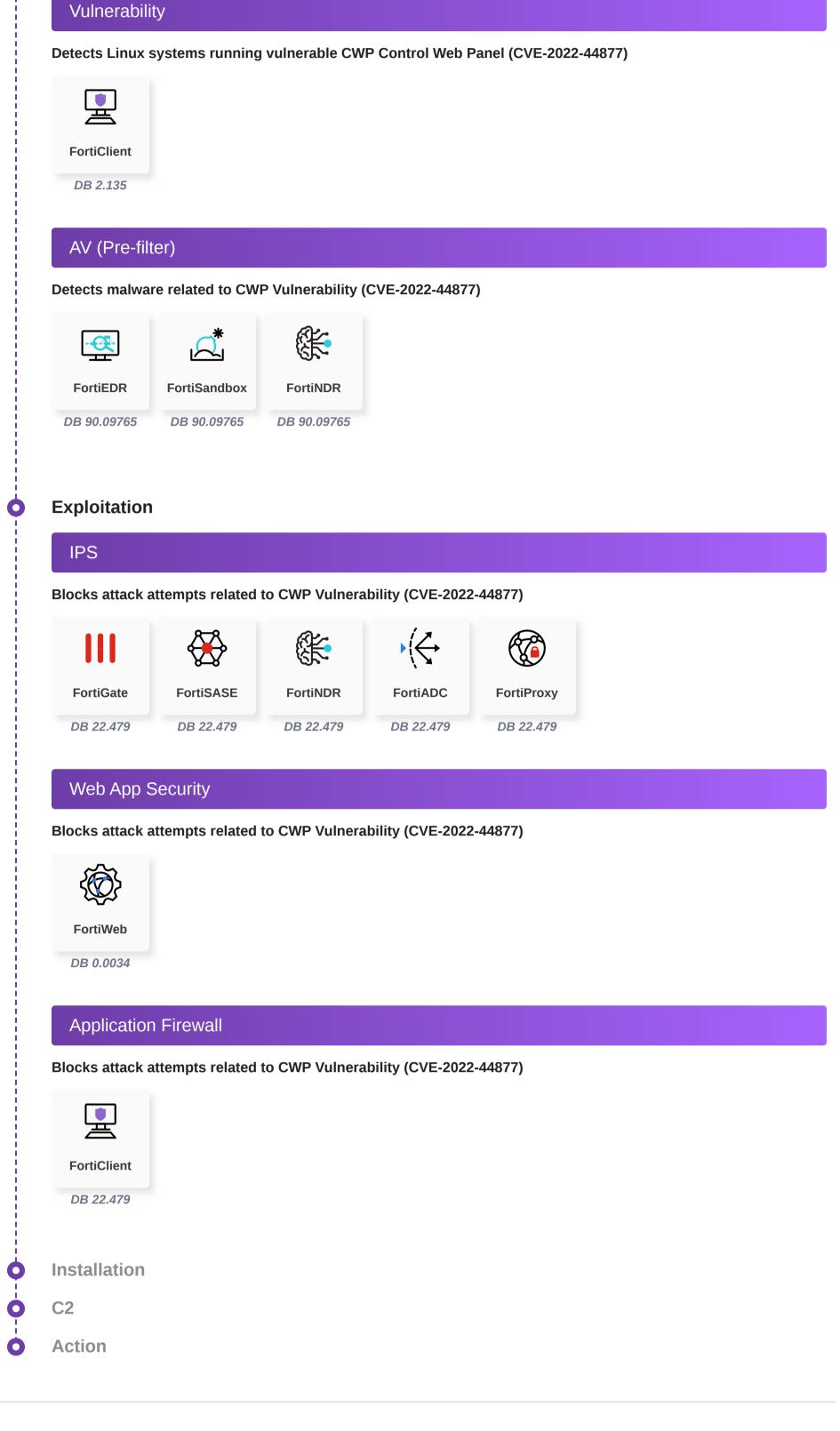
Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Weaponization

#### Delivery





	DETECT
	Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:
•	Outbreak Detection
	Image: DB 1.005Image: DB 1.00084
	IOC
	Image: Non-State State Sta
	Threat Hunting
	Image: Non-AnalyzerImage: Non-AnalyzerV6.4+V6.6+
	Content Update
	V6.6+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automaticlly respond to this outbreak.



FortiXDR

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



## 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

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.



FortiRecon:



Identify processes and assets that need protection:

EASM

**IDENTIFY** 

#### **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

