

C-DATA Web Management System RCE Attack

Critical levels of detections in the wild

<https://github.com/advisories/GHSA-jvx4-vmw6-g8xc>
CVEs: CVE-2022-4257

FortiGuard Labs observed a critical level of attack attempts in the wild targeting a 2-year-old vulnerability found on C-DATA Web Management System.

Background The vulnerability tagged as CVE-2022-4257 allows a remote attacker to execute arbitrary commands on the target system. A remote unauthenticated attacker can send a specially crafted HTTP POST request to the application and execute arbitrary OS commands on the target system. The exploit has been made publicly available; and as of now, we are not aware of any patches available from the vendor.

Latest Developments April 30, 2024: Published the short video.
April 29, 2024: FortiGuard Labs raised the severity from medium to high with the continuous exploitation attempts reaching to almost 50,000 unique IPS devices.
April 25, 2024: FortiGuard Labs observed and blocked attack attempts on 40,000+ unique IPS devices in the week of the release of this outbreak. The majority of the blocked attacks are from IPS devices located in Japan, the United States and Australia.


PROTECT

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

- Reconnaissance
- Weaponization
- Delivery


AV

Detects known malware related to C-DATA Web Management System vulnerability CVE-2022-4257




FortiGate

DB 91.00651




FortiWeb

DB 91.00651




FortiClient

DB 91.00651




FortiSASE

DB 91.00651




FortiMail

DB 91.00651




FortiCASB

DB 91.00651




FortiCWP

DB 91.00651



FortiADC

DB 91.00651




FortiProxy

DB 91.00651


AV (Pre-filter)

Detects known malware related to C-DATA Web Management System vulnerability CVE-2022-4257



FortiEDR

DB 91.00651




FortiSandbox

DB 91.00651

Exploitation


IPS

Detects and blocks attack attempts targeting C-DATA Web Management System RCE




FortiGate

DB 23.535




FortiSASE

DB 23.535




FortiNDR

DB 23.535



FortiADC

DB 23.535




FortiProxy

DB 23.535

Web App Security

Detects and blocks attack attempts targeting C-DATA Web Management System RCE



FortiWeb

DB 0.00375


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




FortiAnalyzer

DB 2.00045




FortiSIEM

v608




FortiSOAR

Threat Hunting




FortiAnalyzer

v6.4+



FortiSIEM

Playbook




FortiSOAR

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.



Incident Response




FortiRecon: ACI

RECOVER


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

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.



NSE Training



Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.



Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening


Check Security Fabric devices to build actionable configuration recommendations and key indicators.



Security Rating

Business Reputation

Know attackers next move to protect against your business branding.



FortiRecon: EASM

Additional Resources

NIST <https://nvd.nist.gov/vuln/detail/CVE-2022-4257>
Exploit DB <https://github.com/siriuswhiter/VulnHub/blob/main/C-Data/rce1.md>

Learn more about [FortiGuard Outbreak Alerts](#)