

Cacti Command Injection Vulnerability

Critical vulnerability exploited in the wild

<https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf>
 CVEs: CVE-2022-46169

In affected versions of Cacti v1.2.22, a command injection vulnerability allows an unauthenticated user to execute arbitrary code on a server running Cacti. Gaining access to the Cacti instance of an organization could give attackers with the opportunity to learn about the types of devices on the network and their local IP addresses.

Background	Cacti is an open source platform which provides a robust and extensible operational monitoring and fault management framework for users.
Announced	December 5, 2022: The patch was released in version 1.2.23 and 1.3.0 on https://github.com/Cacti/cacti/security/advisories/GHSA-6p93-p743-35gf
Latest Developments	February 16, 2023: CISA released advisory and has added CVE-202246169 to its list of known exploited vulnerability (KEV). FortiGuard Labs has already released an IPS signature, in January, to detect and block such attacks and also recommends Cacti admins to patch the vulnerable Cacti versions to 1.2.23, 1.3.0 and above.






PROTECT

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

- Reconnaissance
- Weaponization
- Delivery
- Exploitation


IPS

Detects and Blocks attack attempts related to Cacti Vulnerability (CVE-2022-46169)

 FortiGate DB 22.468	 FortiSASE DB 22.468	 FortiNDR DB 22.468	 FortiADC DB 22.468	 FortiProxy DB 22.468
---	---	--	--	--


Web App Security

Detects and Blocks attack attempts related to Cacti Vulnerability (CVE-2022-46169)

 FortiWeb DB 0.00345

Application Firewall

Detects and Blocks attack attempts related to Cacti Vulnerability (CVE-2022-46169)

 FortiClient DB 22.468

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 1.006	 FortiAnalyzer DB 1.00088
--	--


IOC

 FortiAnalyzer DB 0.02466	 FortiSIEM DB 0.02466	 FortiSOCaaS DB 0.02466
--	--	--

Threat Hunting

 FortiAnalyzer v6.4+	 FortiSIEM v6.6+	 FortiEDR v4.0+
---	---	--

Content Update


 FortiSIEM DB 404
--

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:

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

Threat Signal	https://www.fortiguard.com/threat-signal-report/4937/
Bleeping Computer	https://www.bleepingcomputer.com/news/security/hackers-exploit-cacti-critical-bug-to-install-malware-open-reverse-shells/
SC Magazine	https://www.scmagazine.com/brief/malware/critical-cacti-vulnerability-leveraged-for-malware-deployment
Helpnet Security	https://www.helpnetsecurity.com/2023/01/16/exploiting-cve-2022-46169/
The Hacker News	https://thehackernews.com/2023/01/cacti-servers-under-attack-as-majority.html

Learn more about [FortiGuard Outbreak Alerts](#)