# **OUTBREAK ALERTS**





# 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

**Announced** 

management framework for users.

Cacti is an open source platform which provides a robust and extensible operational monitoring and fault

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

**PROTECT** 



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

Reconnaissance

recommends Cacti admins to patch the vulnerable Cacti versions to 1.2.23, 1.3.0 and above.

Weaponization

events:

Delivery

**Exploitation** 

**IPS** 

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

**FortiGate** DB 22.468

DB 22.468

**FortiSASE** 

**FortiNDR** 

DB 22.468

**FortiADC** DB 22.468

**FortiProxy** DB 22.468

**Application Firewall** 

Web App Security

**FortiWeb** 

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



Installation

DB 0.00345

C2 Action

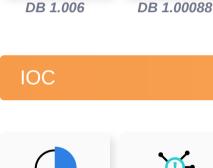
## Outbreak Detection

alert and generate reports:

DETECT

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





**FortiAnalyzer** 



**FortiSIEM** 

**FortiSIEM** 

v6.6+

**FortiSOCaaS** 

DB 0.02466

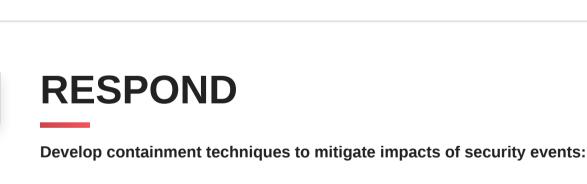
**FortiEDR** 

v4.0+



**Content Update** 





**FortiSIEM** 

**DB 404** 

# **FortiXDR**

Assisted Response Services

**Automated Response** 

FortiRecon:

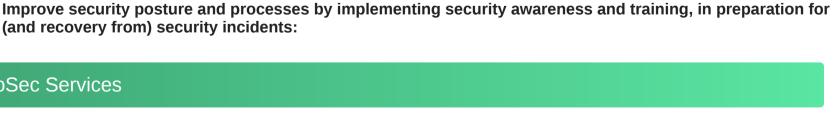
ACI

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

Services that can automatically respond to this outbreak.



Response



Readiness

**IDENTIFY** Identify processes and assets that need protection:

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



**SC Magzine** 

**Helpnet Security** 

Security

Rating

**Additional Resources** 

FortiRecon:

**EASM** 



**FortiDAST** 

#### **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/

The Hacker News https://thehackernews.com/2023/01/cacti-servers-under-attack-as-majority.html

Learn more about FortiGuard Outbreak Alerts



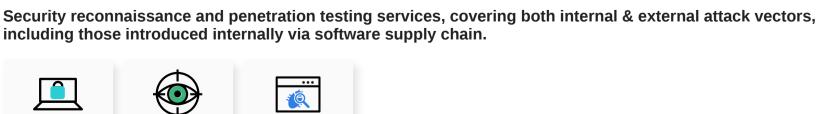
Response

















https://www.scmagazine.com/brief/malware/critical-cacti-vulnerability-leveraged-for-malware-deployment



https://www.helpnetsecurity.com/2023/01/16/exploiting-cve-2022-46169/