F#RTINET. **OUTBREAK ALERTS**



ConnectWise ScreenConnect Attack

An IT remote access tool actively targeted

https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8 CVEs: CVE-2024-1709, CVE-2024-1708

Threat actors including ransomware gangs are seen exploiting newly discovered critical flaws in remote monitoring and management software called ScreenConnect.

Background

could let attackers gain administrative access to a ScreenConnect instance. The second flaw tracked as CVE-2024-1708 is a path traversal vulnerability that may allow an attacker to execute remote code. According to Shadowserver, around 8200 vulnerable ConnectWise ScreenConnect instances were found on the internet and 643 IPs were observed attacking it. According to the company website, ConnectWise remote-access software is one of the leading providers used by

One of the flaws, CVE-2024-1709 is an authentication bypass vulnerability using an alternate path or channel that

threat to end user's systems that could be targeted downstream and can allow hackers to plant malicious code remotely.

Managed service providers (MSPs) to remotely connect to their customer's systems. This could pose a significant

Latest Developments



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

PROTECT

Reconnaissance

FortiClient

DB 91.09996

FortiGate

DB 91.09996

FortiMail

DB 91.09996

FortiProxy

DB 91.09996

Weaponization

Delivery

FortiADC FortiCASB DB 91.09996 DB 91.09996 **FortiSASE FortiWeb**

DB 91.09996 DB 91.09996 **Vulnerability**

Detects end-user devices running the vulnerable application.

DB 1.633

FortiClient

FortiCWP

DB 91.09996

AV (Pre-filter) Detects known malware related to the Outbreak

FortiEDR

DB 91.09996

Exploitation

IPS

DB 91.09996 DB 91.09996

FortiSandbox

FortiNDR

FortiGate

DB 26.740

FortiWeb

Detects and blocks attack attempts leveraging the vulnerability

FortiADC

DB 26.740

Web App Security

Detects and blocks attack attempts leveraging the vulnerability

FortiNDR

DB 26.740

FortiProxy

DB 26.740

FortiSASE

DB 26.740

FortiADC Installation

DETECT

C2 Action

IOC

alert and generate reports:

FortiAnalyzer FortiSOCaaS FortiSIEM

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

FortiClient FortiAnalyzer DB 2.00037 DB 1.0002

Threat Hunting

v2024.2+

FortiEDR

v2024.2+

FortiGate

FortiClient FortiAnalyzer v2024.2+

Automated Response

RESPOND

FortiNDR

Cloud

v2024.2+

Develop containment techniques to mitigate impacts of security events: Services that can automaticlly respond to this outbreak.

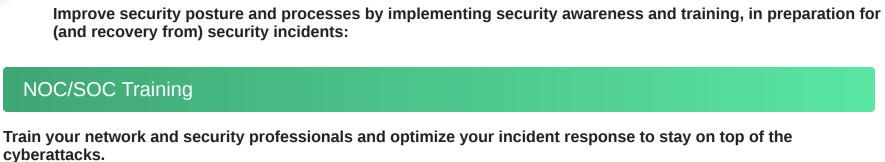
FortiSIEM

v2024.2+

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

FortiXDR

Incident FortiRecon: Response



NSE Training

Awareness &

End-User Training

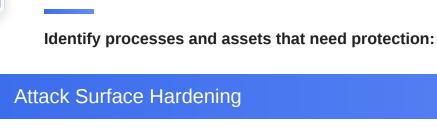
Response

Readiness

RECOVER

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

Training



Security Rating

https://www.helpnetsecurity.com/2024/02/26/cve-2024-1709-exploited/

Reduce the attack surface on software vulnerabilities via systematic and automated patching.



EASM

FortiRecon:

Bleeping Computer https://www.bleepingcomputer.com/news/security/screenconnect-critical-bug-now-under-attack-as-exploit-code-emerges/

Shadowserver https://twitter.com/Shadowserver/status/1760740607268638809

FERTINET.

Learn more about FortiGuard Outbreak Alerts

https://www.darkreading.com/remote-workforce/connectwise-screenconnect-mass-exploitation-delivers-ransomware

Additional Resources

Dark Reading

Helpnet Security

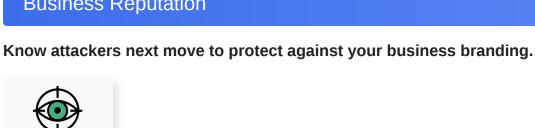
Attack Surface Hardening

IDENTIFY

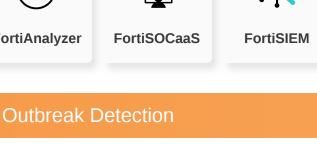
Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Vulnerability Management

FortiClient



Business Reputation



v6.4+