FORTINET

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

One of the flaws, CVE-2024-1709 is an authentication bypass vulnerability using an alternate path or channel that 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 Managed service providers (MSPs) to remotely connect to their customer's systems. This could pose a significant threat to end user's systems that could be targeted downstream and can allow hackers to plant malicious code remotely.

Latest Developments

PROTECT

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

- Reconnaissance
- Weaponization
- **Delivery**

AV

Detects known malware related to the Outbreak

FortiADC	FortiCASB	FortiCWP	FortiClient	FortiGate	FortiMail	FortiProxy
DB 91.09996	*DB 91.09996*	*DB 91.09996*	*DB 91.09996*	*DB 91.09996*	*DB 91.09996*	*DB 91.09996*

FortiSASE	FortiWeb
DB 91.09996	*DB 91.09996*

Vulnerability

Detects end-user devices running the vulnerable application.

FortiClient
DB 1.633

AV (Pre-filter)

Detects known malware related to the Outbreak

FortiEDR	FortiNDR	FortiSandbox
DB 91.09996	*DB 91.09996*	*DB 91.09996*

- **Exploitation**

IPS

Detects and blocks attack attempts leveraging the vulnerability

FortiADC	FortiGate	FortiNDR	FortiProxy	FortiSASE
DB 26.740	*DB 26.740*	*DB 26.740*	*DB 26.740*	*DB 26.740*

Web App Security

Detects and blocks attack attempts leveraging the vulnerability

FortiADC
FortiWeb

- Installation
- C2
- Action

DETECT

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

IOC

FortiAnalyzer
FortiSOCaaS
FortiSIEM

Outbreak Detection

FortiAnalyzer	FortiClient	FortiGate
DB 2.00037	*DB 1.0002*	*v2024.2+*

Threat Hunting

FortiAnalyzer	FortiClient	FortiEDR	FortiNDR Cloud	FortiSIEM
v6.4+	*v2024.2+*	*v2024.2+*	*v2024.2+*	*v2024.2+*

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 targeted 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

Vulnerability Management

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

FortiClient

Business Reputation

Know attackers next move to protect against your business branding.

FortiRecon: EASM

Additional Resources

Dark Reading	https://www.darkreading.com/remote-workforce/connectwise-screenconnect-mass-exploitation-delivers-ransomware
Bleeping Computer	https://www.bleepingcomputer.com/news/security/screenconnect-critical-bug-now-under-attack-as-exploit-code-emerges/
Helpnet Security	https://www.helpnetsecurity.com/2024/02/26/cve-2024-1709-exploited/
Shadowserver	https://twitter.com/Shadowserver/status/1760740607258638809

Learn more about FortiGuard Outbreak Alerts

FORTINET