FORTINET

OUTBREAK ALERTS

ConnectWise ScreenConnect Attack

An IT remote access tool actively targeted

https://community.fortinet.com/t5/FortiEDR/Threat-Coverage-How-FortiEDR-protects-against-post-exploitation/ta-p/303439
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.

Announced

February 19, 2024: ConnectWise published a security advisory and has released a patch covering both vulnerabilities.
https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

February 21, 2024: Proof of Concept (PoC) code was released on GitHub.

February 22, 2024: CVE-2024-1709 was added to CISA's known exploited catalog.
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

February 22, 2024: FortiGuard Labs released a Threat Signal on ConnectWise ScreenConnect Vulnerabilities (CVE-2024-1708 and CVE-2024-1709)
https://www.fortiguard.com/threat-signal-report/5389/

Latest Developments

March 07, 2024: FortiGuard MDR and the FortiGuard IR team responded to several incidents related to exploitation of ConnectWise ScreenConnect and has released a detailed analysis.
https://community.fortinet.com/t5/FortiEDR/Threat-Coverage-How-FortiEDR-protects-against-post-exploitation/ta-p/303439

FortiGuard Labs recommends companies to apply the most recent upgrade or patch from the vendor as soon as possible.

PROTECT

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

Reconnaissance

Lure

Redirect an attacker to engage with a decoy instead of a real ConnectWise ScreenConnect

- FortiDeceptor — v3.3+

Decoy VM

Detects attack attemtps and monitor malicious activities on the network

- FortiDeceptor — v3.3+

Weaponization

Delivery

AV

Detects known malware related to ConnectWise ScreenConnect Attack

- FortiGate — DB 91.09996
- FortiWeb — DB 91.09996
- FortiClient — DB 91.09996
- FortiSASE — DB 91.09996
- FortiMail — DB 91.09996
- FortiCASB — DB 91.09996
- FortiCWP — DB 91.09996
- FortiADC — DB 91.09996
- FortiProxy — DB 91.09996

Vulnerability

Detects vulnerable ScreenConnect software installed on the network (CVE-2024-1708 and CVE-2024-1709)

- FortiClient — DB 1.633

AV (Pre-filter)

Detects known malware related to ConnectWise ScreenConnect Attack

- FortiEDR — DB 91.09996
- FortiSandbox — DB 91.09996
- FortiNDR — DB 91.09996

Exploitation

IPS

Detects and blocks attack attempts targeting ConnectWise ScreenConnect Auth bypass (CVE-2024-1709 & CVE-2024-1708)

- FortiGate — DB 26.740
- FortiSASE — DB 26.740
- FortiNDR — DB 26.740
- FortiADC — DB 26.740
- FortiProxy — DB 26.740

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 1.0002
- FortiAnalyzer — DB 2.00037
- FortiNDR Cloud — v2024.2+

Threat Hunting

- FortiEDR
- FortiAnalyzer — v6.4+
- FortiNDR Cloud — v2024.2+

IOC

- FortiAnalyzer
- FortiSIEM
- FortiSOCaaS

Playbook

- FortiSOAR — v7.4+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automaticlly 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

Vulnerability Management

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

- FortiClient
- FortiEDR

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/1760740607268638809

Learn more about FortiGuard Outbreak Alerts

FORTINET