SECURITY ADVISORY

SEVERE CONNECTWISE SCREENCONNECT VULNERABILITIES

Lodestone Security

FEBRUARY 20TH, 2024

Table of Contents

Executive Summary

On February 19th, 2024, ConnectWise published a security bulletin reporting two impactful vulnerabilities in their product ConnectWise. One of these vulnerabilities is particularly severe, with a critical rating of 10.0 on the CVSS scale, indicating the highest level of risk when successfully exploited.

The two vulnerabilities combined, could allow remote unauthenticated attackers to gain access to ConnectWise SecreenConnect servers. Threat actors can then attempt to leverage this access to target other systems reachable via the ScreenConnect Remote Desktop & Support product.

The vulnerabilities have been replicated by third party security researchers who created a working Proof-of-Concept (PoC) exploit and verified the impact of successful attack. These researchers were able to create a a reliable and functional exploit within just 24 hours of ConnectWise's initial disclosure.

Although widespread exploitation of these vulnerabilities has not yet been observed, the ease of exploitation (showcased by the rapid development of the PoC exploit) and the typical direct internet exposure of the ConnectWise ScreenConnect product suggest a high risk of targeted attacks. Financially motivated threat actors are likely to attempt to quickly develop and deploy weaponized versions of this exploit against publicly accessible ScreenConnect instances in the coming few days.

Lodestone strongly recommends that organizations take **immediate** action to apply the patches highlighted in the “Patches” section of this advisory.

Affected Systems / Products

The following products are reported vulnerable, according to ConnectWise:

- ScreenConnect versions 23.9.7 and prior

Mitigations / Workarounds

No available mitigation or workarounds are currently available; however, ConnectWise has published patches for all impacted versions of the ConnectWise ScreenConnect product.

Lodestone strongly recommends applying available patches immediately.

Patches

These are the patch instructions as given on the ConnectWise site:

Cloud Hosted ScreenConnect Instances

Organizations using ConnectWise-hosted ScreenConnect instances are not required to take any further action. ScreenConnect servers hosted in “screenconnect.com” cloud or “hostedrmm.com” have been updated to remediate the issue.

On-premise Instances

Organizations leveraging on-premise instances of ConnectWise ScreenConnect immediately upgrade their ScreenConnect instances to version 23.9.8 or later in order to address these vulnerabilities.

Recognizing the critical nature of these vulnerabilities, ConnectWise has taken the proactive step of updating previous versions of the ScreenConnect product, specifically from version 22.4 to 23.9.7. Despite these updates, the vendor strongly urges all users to upgrade to ScreenConnect version 23.9.8 at their earliest convenience to ensure the highest level of security and protection against potential exploits.

Additional instructions on applying these security patches are available on ConnectWise's website below:

https://docs.connectwise.com/ConnectWise_ScreenConnect_Documentation/On-premises/Get_started_with_ConnectWise_ScreenConnect_On-Premise/Upgrade_an_on-premises_installation

How Lodestone is Responding

Lodestone has actively identified any instances of ConnectWise ScreenConnect that may be vulnerable within the organizations monitored by Lodestone's Attack Surface Management (ASM) product, Karma.

Sources

- https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8
- https://www.huntress.com/blog/vulnerability-reproduced-immediately-patch-screenconnect-23-9-8