ConnectWise ScreenConnect 23.9.8 security fix

02/19/2024

Products: ScreenConnect

Severity: Critical

Priority: 1 - High

February 27, 2024 update:

Cloud partner summary:
Cloud partners are remediated against both vulnerabilities reported on February 19. No further action is required from any cloud partner ("screenconnect.com" cloud and "hostedrmm.com").

On-prem partner summary:
On-prem partners are advised to immediately upgrade to the latest version of ScreenConnect to remediate against reported vulnerabilities.

Active maintenance
If you are on active maintenance, we strongly recommend upgrading to the most current release of 23.9.8 or later. Using the most current release of ScreenConnect includes security updates, bug fixes, and enhancements not found in older releases.

Off maintenance
ConnectWise has provided a patched version of 22.4.20001 available to any partner regardless of maintenance status as an interim step to mitigate the vulnerability. If you are not currently under maintenance, please upgrade your servers to version 22.4.20001 at minimum or to your latest eligible patched version that includes the remediation for CVE-2024-1709.

(Updated) Addressing license errors: If a license error arises during the upgrade, please stop the four ScreenConnect services (Session Manager, Security Manager, Web Server, Relay), move the "**License.xml"** file from the installation folder "**C:\Program Files (x86)\ScreenConnect\App_Data\License.xml**" to another location such as Desktop, and proceed with the upgrade. After the upgrade is complete, the license key will need to be re-added by stopping the four services and dropping the file back into the App_Data folder.

Active Advisory

- Unauthenticated access to legacy AWS server located in the EU region
- ScreenConnect vulnerability CWE-288
- ScreenConnect 23.9.8 security bulletin
- How to upgrade on-premise installation
- Remediation + Hardening Guide (pdf)

Helpful Links

- Advisories RSS feed link
- Chrome RSS feed extension
- Visit our Trust Center
- See latest security bulletins
- Check status.connectwise.com
- Call 1-888-WISE911 to report a security vulnerability
- @connectwise.com
- open a ticket on ConnectWise Home
- eck my email preferences

ICYMI: ConnectWise has taken an exception step to support partners no longer under maintenance by making them eligible to install version 22.4 at no additional cost, which will fix CVE-2024-1709, the critical vulnerability. However, this should be treated as an interim step. ConnectWise recommends on-premise partners upgrade to remain within maintenance to gain access to all security and product enhancements.

February 22, 2024 update:

ConnectWise recommends on-premise partners immediately update to 23.9.8 or higher to remediate reported vulnerabilities. ConnectWise has rolled out an additional mitigation step for unpatched, on-premise users that suspends an instance if it is not on version 23.9.8 or later. If your instance is found to be on an outdated version, an alert will be sent with instructions on how to perform the necessary actions to release the server.

To upgrade your version to our latest 23.9 release, please follow this upgrade path:

2.1 → 2.5 → 3.1 → 4.4 → 5.4 → 19.2 → 22.8 → 23.3 → 23.9

If you need any assistance or have additional questions, please go online to ConnectWise Home and open a case with our support team or email help@connectwise.com.

February 21, 2024 update*:

Cloud partner summary: Cloud partners are remediated against both vulnerabilities reported on February 19. No further action is required from any cloud partner ("screenconnect.com" cloud and "hostedrmm.com").

On-prem partner summary: On-prem partners are advised to immediately upgrade to the latest version of ScreenConnect to remediate against reported vulnerabilities.

Today, ScreenConnect version 23.9.10.8817 was released containing a number of fixes to improve customer experience. It is always recommended to be on the latest version but 23.9.8 is the minimum version that remediated the reported vulnerabilities.

As part of this release, ConnectWise has removed license restrictions, so partners no longer under maintenance can upgrade to the latest version of ScreenConnect.

**Please see the February 27, 2024 security bulletin update that clarifies partners off maintenance can upgrade to 22.4.20001 (or a later eligible version) to receive a patch to CVE-2024-1709. To get the current 23.9.8 or later release, partners need to be on active maintenance.*

February 20, 2024 update:

Indicators of compromise
Indicators of compromise (IOCs) look for malicious activity or threats. These indicators can be incorporated into your cybersecurity monitoring platform. They can help you stop a cyberattack that's in progress. Plus, you can use IOCs to find ways to detect and stop ransomware, malware, and other cyberthreats before they cause data breaches.

We've received notifications of suspicious activity that our incident response team has investigated. The following IP addresses were used by threat actors. We are making them available for protection and defense.

IOCs:

- 155.133.5.15
- 155.133.5.14
- 118.69.65.60

We will continue to update with any further information as it becomes available.

Original Bulletin:

ure channel via the ConnectWise Trust Center.
t immediate action must be taken by on-

- CWE-288 Authentication bypass using an alternate path or channel
- CWE-22 Improper limitation of a pathname to a restricted directory ("path traversal")

CWE ID	Description	Base Score	Vector
CWE-288	Authentication bypass using an alternate path or channel	10	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE-22	Improper limitation of a pathname to a restricted directory ("path traversal")	8.4	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H

Severity

Critical—Vulnerabilities that could allow the ability to execute remote code or directly impact confidential data or critical systems.

Priority

1 High—Vulnerabilities that are either being targeted or have higher risk of being targeted by exploits in the wild. Recommend installing updates as emergency changes or as soon as possible (e.g., within days)

Affected versions

ScreenConnect 23.9.7 and prior

Remediation

Cloud

There are no actions needed by the partner, ScreenConnect servers hosted in "screenconnect.com" cloud or "hostedrmm.com" have been updated to remediate the issue.

On-premise

Partners that are self-hosted or on-premise need to update their servers to version 23.9.8 immediately to apply a patch.

ConnectWise will also provide updated versions of releases 22.4 through 23.9.7 for the critical issue, but strongly recommend that partners update to ScreenConnect version 23.9.8.

For instructions on updating to the newest release, please reference this doc: Upgrade an on-premise installation - ConnectWise

Link to patch: Download | ConnectWise ScreenConnect™

FAQs

Frequently asked questions

^ What happened?

On February 13, 2024, an independent researcher ethically and responsibly reported two potential vulnerabilities using Trust Center, including a potential critical on bypass flaw to create admin accounts on stem admin, delete all other users and take

- What is the current status of the vulnerability?
- How can partners protect themselves?
- What's the state of hosted/cloud partners?
- For cloud partners, do we need to make sure that all devices have been patched?
- Why was cloud patched first? Why was there a gap between patching the cloud and notifying on-prem partners?
- Version 23.9.10 was released, do I need to be on that version?
- What can I do if I suspect I have been compromised?
- I'm considering migrating/have migrated my on-prem server to ScreenConnect cloud since the security bulletin. What should I consider as part of a cloud migration?
- Some of the partners are getting a license revoked error, even after upgrading their server to the latest version and rebooting. What do we do next?
- Do my agents need to be upgraded? Were my agents affected by the vulnerability? Some security tools are flagging ScreenConnect agents as malware.
- Why didn't I receive an email? Who at my company did receive an email?
- How do I get added to future security communications and important notices from ConnectWise?
- Why was my cloud-hosted ScreenConnect showing a version older than 23.9.8 when the security advisory said we had already been updated?
- Why did my cloud-hosted ScreenConnect instance have downtime on February 21?
- How do I know what version of ScreenConnect I am eligible for?
- What happens once I have patched to a remediated version?
- Do these vulnerabilities directly affect ScreenConnect clients?
- Is there any connection between the ConnectWise ScreenConnect vulnerability disclosed on February 19, 2024, and the incident at Change Healthcare?
- What is ConnectWise doing to prevent vulnerabilities or exploits from happening again?
- How do I report a security incident?
- Where can partners go for more information and support?