BUSINESS SOFTWARE - IT MANAGEMENT – PROCESS CONSULTING – CYBER SECURITY

# ConnectWise ScreenConnect Vulnerabilities

## February 2024

SOC Informative Report

# Document details

## Title of the activity

ConnectWise ScreenConnect Vulnerabilities

## Summary

Report containing information about two (CVE-2024-1708 and CVE-2024-1709) vulnerabilities for ConnectWise ScreenConnect, categorized as *Authentication bypass using an alternate path or channel* and *Improper limitation of a pathname to a restricted directory.*

## Target audience

SOC and SOC AdS representatives

## Confidentiality level (Clear/Green/Amber/Amber+Strict/Red)

CLEAR

## Publication date

22/02/2024

## Written by

Luca Zeni

## Reviewed by

Massimo Giaimo

# Confidentiality level

A level of confidentiality is applied to the document, marked by the "Confidentiality Level" item on the front page. The values that can be used (RED / AMBER / AMBER+STRICT / GREEN / CLEAR) have the following meanings:

**TLP:RED** = Reserved for participants only.

Sources may use TLP:RED when the information cannot be effectively used by other parties and could impact a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with parties outside the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most cases, TLP:RED should be exchanged verbally or in person.

**TLP:AMBER** = Limited disclosure, restricted to participants' organizations.

**TLP:AMBER+STRICT** limits sharing to the *organization* only.

Sources may use TLP:AMBER when the information requires support to act effectively but poses risks to privacy, reputation, or operations if shared outside the organizations involved. Recipients may share TLP:AMBER information only with members of their own organization and with clients or customers who need to know the information to protect themselves or prevent further harm.

Note: If the source wishes to limit sharing **only** to the organization, it must specify TLP:AMBER+STRICT.

**TLP:GREEN** =Limited disclosure, restricted to the community.

Sources may use TLP:GREEN when the information is useful for the awareness of all participating organizations, as well as with colleagues within the community or broader sector. Recipients may share TLP:GREEN information with colleagues and partner organizations within their sector or community, but not through publicly accessible channels. Information in this category may be widely disseminated within a particular community. TLP:GREEN information may not be released outside the community.

**TLP:CLEAR** = Disclosure is not limited.

Sources may use TLP:CLEAR when the information poses little or foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.

# Table of contents

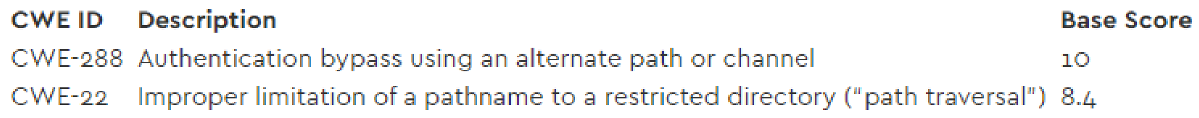
# Introduction

**ConnectWise ScreenConnect** is a remote desktop software solution popular with help desk teams. The product is offered as cloud-hosted software-as-a-service or can be deployed by organizations as a self-hosted server application.

This software has gained popularity in recent years among tech support scammers and various cybercriminals, including ransomware gangs. To prevent fraudsters from creating their own branded service portals and tricking employees into participating in malicious remote access sessions, ConnectWise disabled the personalisation function for trial accounts of its cloud-hosted service at the end of 2022.

ConnectWise announced on **February 13, 2024**, the identification of two vulnerabilities (CVE-2024-1708[1] and CVE-2024-1709[2]) in their remote access tool, and on **February 19, 2024** released a security fix.

These vulnerabilities directly impact and target on-prem or self-hosted ScreenConnect Web Servers running version 23.9.7 and prior.



| CWE ID | Description | Base Score |
|---|---|---|
| CWE-288 | Authentication bypass using an alternate path or channel | 10 |
| CWE-22 | Improper limitation of a pathname to a restricted directory ("path traversal") | 8.4 |

*ConnectWise Original Bulletin* [3]

# Overview of the attack

As already mentioned, the ScreenConnect software was affected by two vulnerabilities:

- Authentication bypass using an alternate path or channel (CVE-2024-1709 - *CVSS score: 10.0*)
- Improper limitation of a pathname to a restricted directory (CVE-2024-1708 - *CVSS score: 8.4*)

The initial vulnerability, disclosed with a baseline critical CVSS score of 10 (the highest possible severity), involved an authentication bypass which, in turn, would open the way for the second vulnerability with a CVSS score of 8.4.

Even though there is currently no evidence that these vulnerabilities have been exploited, ConnectWise indicates a high risk of potential exploits targeting these vulnerabilities.

It is currently not possible to provide a detailed overview of the attack. However, an examination of the differences between the latest version of the binaries and the previous unpatched version reveals a new check implemented to ensure correct configuration before granting the user access to the configuration wizard.

Various groups have classified these exploits as "trivial and embarrassingly easy"

Researchers from Horizon3 have presented essential evidence of a Proof-of-Concept (PoC)[4], but they are not alone, as other vendors are now publicly sharing information about the exploit.

In addition, as evidence of the attack's viability, a particular PoC exploit has been publicly released in the last few hours and is currently accessible.

Concerns about these vulnerabilities have increased considerably. The increased concern stems primarily from the possibility of attackers exploiting vulnerable instances of ScreenConnect to subsequently distribute ransomware to downstream clients

# Remediation

The affected versions of the product are the 23.9.7 and prior.

**Cloud:**

- The partner does not need to take any action as the ScreenConnect servers hosted in the "screenconnect.com" cloud or "hostedrmm.com" have already been updated to resolve the issue.

**On-premise**

- Self-hosted or on-premise partners should promptly update their servers to version 23.9.8 to implement a necessary patch. [5]

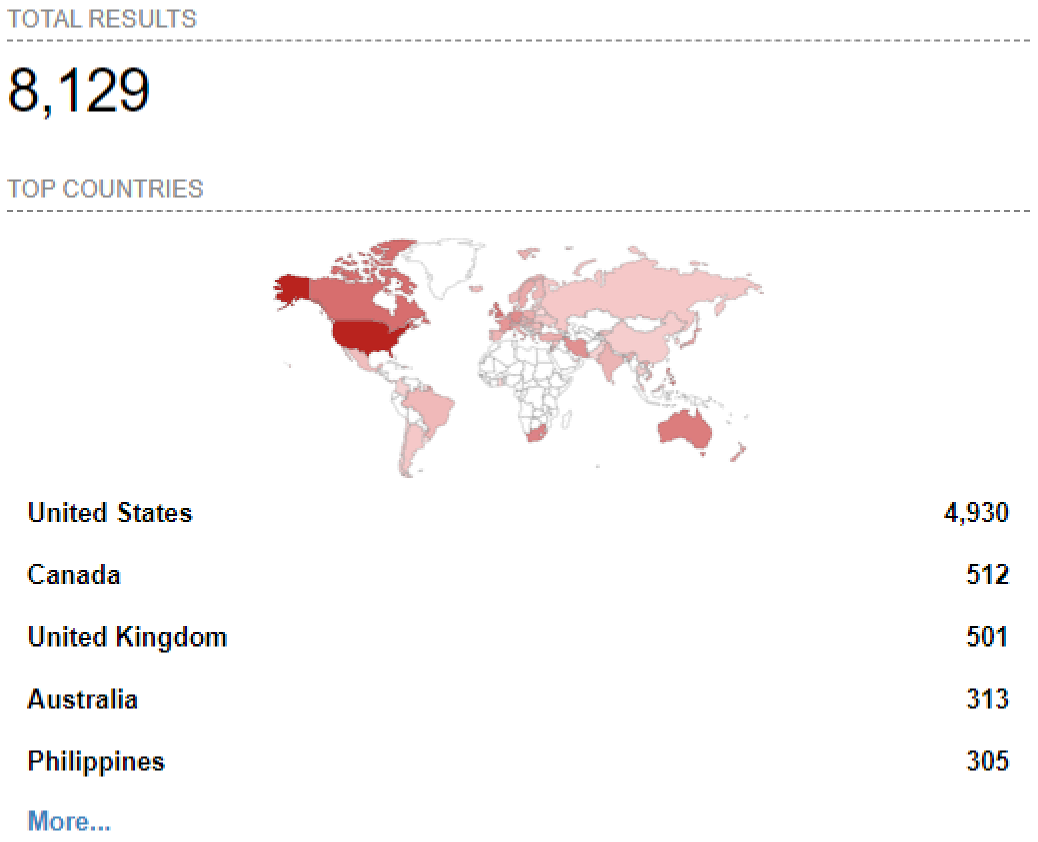
ConnectWise will also provide updated versions of releases 22.4 through 23.9.7 for the critical issue, but strongly recommend that partners update to ScreenConnect version 23.9.8.

# Attack surface

Using a device search engine such as **Shodan**, it is possible to check the amount of servers running a vulnerable version of ScreenConnect on the Internet and are publicly reachable.

Below are the devices found with the Shodan query ("Server: ScreenConnect", search date 21/02/2024):

| **Shodan Query** |
|---|
| ScreenConnect |



TOTAL RESULTS

8,129

TOP COUNTRIES

| | |
|---|---|
| United States | 4,930 |
| Canada | 512 |
| United Kingdom | 501 |
| Australia | 313 |
| Philippines | 305 |

More...

# Detection

The following detection rules are available:

https://github.com/SigmaHQ/sigma/tree/master/rules-emerging-threats/2024/Exploits/CVE-2024-1708

https://github.com/SigmaHQ/sigma/tree/master/rules-emerging-threats/2024/Exploits/CVE-2024-1709

# IOCs

- *IP addresses:*
  - *155.133.5.15*
  - *155.133.5.14*
  - *118.69.65.60*

# Bibliography

[1] https://nvd.nist.gov/vuln/detail/CVE-2024-1708

[2] https://nvd.nist.gov/vuln/detail/CVE-2024-1709

[3]https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

[4]https://twitter.com/horizon3attack/status/1760019078280826903?s=46&t=-dkNDSDHEzyAagaVN0SDgA

[5]https://screenconnect.connectwise.com/download