

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.

Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Privacy Policy](#)

Manage Preferences

Accept All

Reject All

Collapse all

Required CVE Record Information

CNA: Cybersecurity And Infrastructure Security Agency (CISA) U.S. Civilian Government

Published: 2024-02-21Updated: 2024-02-21

Title: Authentication Bypass Using An Alternate Path Or Channel

Description

ConnectWise ScreenConnect 23.9.7 and prior are affected by an Authentication Bypass Using an Alternate Path or Channel vulnerability, which may allow an attacker direct access to confidential information or critical systems.

CWE1 Total

[Learn more](#)

- CWE-288: CWE-288 Authentication bypass using an alternate path or channel

CVSS1 Total

[Learn more](#)

Score	Severity	Version	Vector String
10.0	CRITICAL	3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/

Product Status

[Learn more](#)

Vendor

ConnectWise

Product

ScreenConnect

Versions1 Total

Default Status: unaffected

Affected

- affected from 0 through 23.9.7
 - unaffected from 23.9.8

References

On This Page

Required CVE Record Information

CNA: Cybersecurity And Infrastructure Security Agency (CISA) U.S. Civilian Government

CVE Program

Authorized Data Publishers

CISA-ADP

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Privacy Policy](#)

[-bypass-add-user-poc](#)

- <https://github.com/rapid7/metasploit-framework/pull/18870>
- <https://www.horizon3.ai/attack-research/red-team/connectwise-screenconnect-auth-bypass-deep-dive/>
- <https://techcrunch.com/2024/02/21/researchers-warn-high-risk-connectwise-flaw-under-attack-is-embarrassingly-easy-to-exploit/>
- <https://www.securityweek.com/connectwise-confirms-screenconnect-flaw-under-active-exploitation/>
- <https://www.huntress.com/blog/a-catastrophe-for-control-understanding-the-screenconnect-authentication-bypass>

CVE Program

Updated: 2024-08-01

This container includes required additional information provided by the CVE Program for this vulnerability.

References

- <https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8>
x_transferred
- <https://www.huntress.com/blog/vulnerability-reproduced-immediately-patch-screenconnect-23-9-8>
x_transferred
- <https://www.huntress.com/blog/detection-guidance-for-connectwise-cwe-288-2>
x_transferred
- <https://www.bleepingcomputer.com/news/security/connectwise-urges-screenconnect-admins-to-patch-critical-rce-flaw/>
x_transferred
- https://github.com/watchtowrlabs/connectwise-screenconnect_auth-bypass-add-user-poc
x_transferred
- <https://github.com/rapid7/metasploit-framework/pull/18870>
x_transferred
- <https://www.horizon3.ai/attack-research/red-team/connectwise-screenconnect-auth-bypass-deep-dive/>
x_transferred
- <https://techcrunch.com/2024/02/21/researchers-warn-high-risk-connectwise-flaw-under-attack-is-embarrassingly-easy-to-exploit/>
x_transferred
- <https://www.securityweek.com/connectwise-confirms-screenconnect-flaw-under-active-exploitation/>
x_transferred

To improve your experience, we (and our partners) store and/or access information on your terminal (cookie or equivalent) with your consent for all our websites and applications, on your connected terminals.
Our website may use these cookies to:

- Measure the audience of the advertising on our website, without profiling
- Display personalized ads based on your navigation and your profile
- Personalize our editorial content based on your navigation
- Allow you to share content on social networks or platforms present on our website
- Send you advertising based on your location

[Privacy Policy](#)

CISA-ADP

+

Policies & Cookies

- Terms of Use
- Website Security Policy
- Privacy Policy
- Cookie Notice
- Manage Cookies




Media




- News
- Blogs
- Podcasts
- Email newsletter sign up

Social Media

- 
-  New CVE Records
 -  CVE Announce

Contact

- CVE Program Support 
- CNA Partners
- CVE Website Support 
- CVE Program Idea Tracker 

Use of the CVE[®] List and the associated references from this website are subject to the [terms of use](#). CVE is sponsored by the [U.S. Department of Homeland Security \(DHS\)](#)  [Cybersecurity and Infrastructure Security Agency \(CISA\)](#) . Copyright © 1999-2024, [The MITRE Corporation](#) . CVE and the CVE logo are registered trademarks of The MITRE Corporation.