National Cyber Security Centre

2402200123-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical and High Severity Vulnerabilities in ConnectWise ScreenConnect

UPDATE

Thursday 22nd February, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Revision History

Revision	Date	Author(s)	Description
1.0	19th Febuary 2024	CSIRT-IE	Initial advisory
1.1	22nd Febuary 2024	CSIRT-IE	Update with CVE numbers and IOCs

Description

ConnectWise has released software updates to address two vulnerabilities in its ScreenConnect remote desktop and access software. CVE numbers to be confirmed. The vulnerabilities are as follows:

- CVE-2024-1709: Authentication bypass using an alternate path or channel (CVSS 3.1 score: **10.0**)
- CVE-2024-1708: Improper limitation of a pathname to a restricted directory aka "path traversal" (CVSS 3.1 score: **8.4**)

Exploitation of these could allow the ability to execute remote code or directly impact confidential data or critical systems.

Products Affected

The following ConnectWise products are affected:

- ScreenConnect 23.9.7 **and prior.**

Impact

Exploitation of these could allow the ability to execute remote code or directly impact confidential data or critical systems.

The NCSC is aware that these vulnerabilities are being actively exploited.

Indicators Of Compromise

IOC	Description
155.133.5[.]15	IP address observed by ConnectWise incident response team
155.133.5[.]14	IP address observed by ConnectWise incident response team
118.69.65[.]60	IP address observed by ConnectWise incident response team

Recommendations

Organisations that are self-hosted or on-premise need to update their servers to version 23.9.8 immediately.

There are no actions needed by organisations who run cloud versions - ConnectWise have said ScreenConnect servers hosted in “screenconnect.com” cloud or “hostedrmm.com” have been updated to remediate the issue.

The NCSC strongly advises affected organisations to identify any assets that are running the affected ScreenConnect versions and apply the updates recommended by ConnectWise in their advisory.

Further information from ConnectWise including instructions on updating to the newest release can be found here: https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie