An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2609100235

NCSC Advisory

Critical Vulnerability in ConnectWise ScreenConnect

CVE-2026-84869

10th, September 2026

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.

Description

CVE ID: CVE-2026-84869

Published: 2026-09-08

Vendor: ConnectWise

Product: ScreenConnect

CVSS Score[1]: 9.9

Products Affected

Product	Version
ScreenConnect	All versions prior to 26.6.5

Impact

A condition in the ScreenConnect client may allow files to be transferred and executed through an active remote session without authorization or Host confirmation in certain circumstances. ScreenConnect servers are not impacted.

Common Weakness Enumeration (CWE)[2]: CWE-862 Missing Authorization, CWE-269 Improper Privilege Management

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from ConnectWise.

- https://nvd.nist.gov/vuln/detail/CVE-2026-84869
- https://www.cve.org/CVERecord?id=CVE-2026-84869
- https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin
- https://www.connectwise.com/company/trust/advisories