

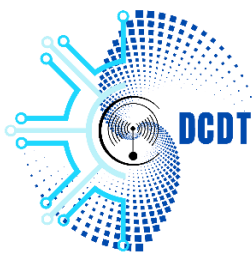
**GOVERNMENT OF THE REPUBLIC
OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380



**GOUVERNEMENT DE LA
REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu

Tel: (678) 33380

14 September 2026

Advisory 305: ConnectWise ScreenConnect Client Unauthorized File Transfer and Execution — Actively Exploited (CVE-2026-84869).

Release Date: 14th September 2026

Impact: **CRITICAL**

TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations, Managed Service Providers, and System/Network administrators that operate a ConnectWise ScreenConnect client for remote support or remote access. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-84869 is a critical vulnerability in the ConnectWise ScreenConnect client, one of the world's most widely-used remote support and remote access tools, deployed by managed service providers, IT help desks, and organizations of every size globally to remotely access and support end-user and server systems. A condition in the ScreenConnect client allows files to be transferred to, and executed on, the host computer through an active remote session without authorization or Host confirmation in certain circumstances — bypassing the confirmation prompt a host user would normally be shown before a remote party can push and run a file on their machine. Only ScreenConnect clients are affected; ScreenConnect servers are not. ConnectWise first warned customers of the issue on 3 September 2026 and released a fix five days later, on 8 September 2026, in ScreenConnect client version 26.6.5. ScreenConnect has a well-documented history of being targeted for initial access and ransomware deployment (including a prior nation-state campaign and separately-exploited vulnerabilities), making any unauthorized file-execution flaw in the product a high-value target for attackers.

The vulnerability is tracked under CWE-269 (Improper Privilege Management) and, per one tracker, also CWE-862 (Missing Authorization), and is independently corroborated by three separate third-party trackers (Strix, TheHackerWire, and Vulners) with full agreement: CVSS v3.1 9.9 (Critical) — CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H — reflecting a network-exploitable flaw with a scope change to the underlying host system. This vulnerability is confirmed under active exploitation and has been added to CISA’s Known Exploited Vulnerabilities catalog, with U.S. federal agencies required to remediate by 14 September 2026. Given confirmed active exploitation, the maximum-practical impact of unauthorized file execution on a remote-support host, and the product’s established history as a ransomware-deployment vector, this is an emergency, same-day patching priority for any organization running ScreenConnect clients.

What are the systems affected?

The following version(s) are affected:

- ConnectWise ScreenConnect client, versions prior to 26.6.5.9742 – (Affected)

ConnectWise ScreenConnect client, version 26.6.5.9742 and later – (Not affected, patched);
ScreenConnect servers are not affected by this vulnerability

Upgrade every ScreenConnect client to version 26.6.5.9742 or later without delay. Where immediate patching is not possible, ConnectWise’s published interim workaround is to manually remove the “TransferFiles” permission from active user sessions until the upgrade can be applied.

What does this mean?

Typical attack flow:

1. **Establish or hijack an active ScreenConnect remote session**
 - An attacker with access to an active ScreenConnect remote session — for example, a malicious or compromised “guest”/technician-side party — attempts to transfer a file to the host machine being remotely supported or accessed.
2. **Transfer and execute the file on the host without authorization or confirmation**
 - Due to the flawed condition in the ScreenConnect client, the file transfer and execution succeed without the Host confirmation prompt that should normally require the host user’s explicit approval, letting the attacker run arbitrary code on the host system.

Attack vectors:

- An attack against any active ScreenConnect remote-support or remote-access session, most critically where the ScreenConnect client is used to provide third-party or managed-service-provider support, or where session access itself has already been compromised.
- No user interaction beyond an already-active session is required for the file transfer/execution step itself (CVSS UI:N), and only low privileges are needed to trigger it (CVSS PR:L) once session access exists. This is confirmed under active exploitation and is listed in CISA’s KEV

catalog — this is not a theoretical risk, and any unpatched ScreenConnect client should be treated as a priority remediation target.

Successful exploitation may allow attackers to:

- Transfer and execute arbitrary files on a host system through an active ScreenConnect remote session, without the authorization or confirmation the product is designed to require.
- Use that unauthorized code execution to establish persistence, deploy further malware or ransomware, and pivot into the wider network the host system is connected to — consistent with ScreenConnect's established history as a targeted initial-access and ransomware-deployment vector.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch immediately

- Upgrade every ScreenConnect client to version 26.6.5.9742 or later as an emergency change, not scheduled maintenance, given confirmed active exploitation and the CISA KEV federal remediation deadline of 14 September 2026.

2. Apply the interim workaround where patching must be delayed

3. Audit ScreenConnect sessions and connected systems for signs of prior compromise

- Review ScreenConnect session logs and file-transfer history for unexpected or unauthorized file transfers to host systems, and treat any host that participated in an unpatched session during an active remote-support engagement as warranting closer inspection.

4. Confirm coverage across every client, not just the server

- Because this vulnerability affects ScreenConnect clients specifically (not servers), organizations — particularly managed service providers supporting many end-customer environments — should confirm the patch has reached every deployed client, not only the central ScreenConnect server instance.

5. Report suspected compromise

Report any suspected compromise involving a ScreenConnect session to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. <https://www.cve.org/CVERecord?id=CVE-2026-84869>
2. <https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin>