ConnectWise ScreenConnect guest-to-technician payload execution in client (CVE-2026-84869)

Status: Recovering / monitoring

Started Nov 28, 2026, 11:31 AM PST · ConnectWise's estimate: Fixed versions are available

CVE-2026-84869 · CVSS 9.9 (critical) · Being exploited: yes · Fix available: yes

WHAT'S HAPPENING

ScreenConnect is remote-support software that IT providers use to connect to customers' computers. Normally the technician decides which files are transferred and run during a session. Because of this flaw, a malicious guest could send a file to the technician's computer and have the technician's own ScreenConnect client run it, without approval. Researchers say attackers used this against IT service providers (MSPs). They joined sessions as fake guests, pushed scripts, and installed a disguised remote-access client that they controlled. ConnectWise published a fix on September 8, 2026. It says the ScreenConnect server is not affected and that cloud-hosted instances were already updated. Older technician clients still need to be updated, and some were reportedly still in use weeks after the fix.

WHO IS AFFECTED

- ScreenConnect host (technician) clients before version 26.6.5, for both cloud and on-premises deployments
- Access agents that ConnectWise lists in its security bulletin, before version 26.6.5
- IT providers and internal IT teams whose technicians join guest sessions. Their customers could be affected indirectly if a technician's computer is compromised.
- Not affected, per ConnectWise: the ScreenConnect server itself

IS IT BEING EXPLOITED?

CISA added CVE-2026-84869 to its Known Exploited Vulnerabilities list on September 11, 2026, according to secondary reports. Security firm Huntress reported a November 12, 2026 attack in which a technician's workstation ran an attacker's file and started a rogue remote-access client in about 9 seconds. I could not open CISA's own entry, so the KEV date comes from news and research sites. Public reporting reviewed did not name a specific attacker group.

WHAT YOU SHOULD DO NOW

Home users

- You most likely don't need to do anything yourself unless you run ScreenConnect. This mainly affects the technicians' computers.
- If an IT provider supports your computers, ask whether they have updated all technician ScreenConnect clients to 26.6.5 or later.
- Only accept remote-support sessions you requested. Be wary of unexpected calls, pop-ups or "tech support" contacts asking you to install remote-access software.
- If you installed a ScreenConnect client yourself, update it to 26.6.5 or later. If you don't recognize a ScreenConnect or remote-access program on your computer, ask a trusted IT professional to check it.
- Keep Windows and your security software up to date.

Businesses

- Update every technician's ScreenConnect host client, and any Access agents listed in ConnectWise's bulletin, to 26.6.5 or later. Updating the server or cloud instance alone is not enough.
- Use your server's connection history to find clients that still connect with older versions.
- If you can't update right away, ConnectWise's temporary mitigation is to remove the TransferFiles permission

from roles and session groups. This is per secondary reports of the bulletin. Confirm it in ConnectWise's bulletin.

- Look for signs of compromise on technician computers. These include guest-pushed files named update.bat or update_ followed by 8 characters, unfamiliar ScreenConnect clients (for example one disguised as a Windows update), and connections to unknown relay servers. Reported indicators include the domain masterdarky[.]com.
- If you find signs of compromise, isolate the computer, rotate technician and admin credentials, and end active sessions. Consider professional incident response.
- Turn on multi-factor authentication for all ScreenConnect accounts, and restrict access to trusted networks where possible.
- If an outside IT provider supports you, ask them in writing whether their technician clients are patched.

HOW TO CHECK IF YOU'RE AFFECTED

- Self-hosted server admins: open the ScreenConnect Administration page and look at the Support/Access session connection history for each client's version number.
- On a Windows technician computer: open Settings > Apps > Installed apps (or Control Panel > Programs and Features) and find ScreenConnect Client. Check the version. It should be 26.6.5 or later.
- Check the ConnectWise security bulletin "ScreenConnect 26.6.5 Security Patch" (dated September 8, 2026) for the exact list of affected clients and agents.
- Reported exact build numbers differ between sources (for example 26.6.5.9742). Rely on the ConnectWise bulletin for the precise build.

FIXED VERSIONS AND WORKAROUNDS

- ConnectWise ScreenConnect host client and listed Access agents: 26.6.5 or later

Until you can update:

- Temporary mitigation reported from ConnectWise's bulletin: remove the TransferFiles permission from roles and session groups until you can update.
- Enforce multi-factor authentication, rotate technician credentials, and limit access to trusted IP ranges. These are general hardening steps from security vendors, not a replacement for patching.

OTHER COVERAGE

The Hacker News: Hackers Exploit Critical ScreenConnect Flaw to Hijack MSP Technician PCs Without Warning — https://thehackernews.com/2026/11/hackers-exploit-critical-screenconnect.html

SOCRadar: ScreenConnect Flaw CVE-2026-84869 Exploited — https://socradar.io/blog/screenconnect-cve-2026-84869-exploitation/

Arctic Wolf: CVE-2026-84869 ConnectWise ScreenConnect Client Vulnerability — https://arcticwolf.com/resources/blog/cve-2026-84869/

Ostorlab: ScreenConnect Client RCE Exploited in the Wild (CVE-2026-84869) — https://blog.ostorlab.co/screenconnect-client-rce-cve-2026-84869.html

ABOUT THIS BRIEF

Last updated November 28, 2026. Researched with AI help from public sources and checked against the official advisories above. Details can change; follow your vendor's guidance.

Questions? Contact BIS Computer Solutions, Inc.

5500 Alta Canyada Rd., La Canada, CA 91011 USA · Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com