ScreenConnect Flaw CVE-2026-84869 Exploited Against MSP Technician Hosts



Attackers are exploiting CVE-2026-84869 (CVSS 9.9), a patched critical flaw in the ConnectWise ScreenConnect client, to run malicious payloads on technicians' machines connecting to a guest session.

- CVE-2026-84869 carries a CVSS score of 9.9 and affects the ScreenConnect client.
- A guest can transfer and run a malicious payload on the host of a technician who connects.
- Managed service provider (MSP) servers are among the reported targets.
- The flaw has been patched, and exploitation has been observed in the wild.
- The source reports an observed incident on November 12, 2026.

Threat actors are exploiting a critical vulnerability in ConnectWise ScreenConnect, tracked as CVE-2026-84869 and rated 9.9 on the CVSS scale. The vendor has already released a fix, but attacks against managed service provider environments have been observed.

What happens

The flaw sits in the ScreenConnect client. A guest, meaning the remote party in a support session, can transfer a malicious payload to the technician's host and have it executed when the technician connects. The direction of risk is therefore reversed from the usual pattern: the support engineer's own workstation becomes the target, not the customer's.

The source describes an incident observed on November 12, 2026, involving a managed service provider. It does not give further details in the portion available, so the scope of the campaign and the identity of the actors remain unclear.

Why it matters for Saudi institutions

Technician workstations typically hold privileged access to many client environments. A compromise there can become a route into several organisations at once. Regulated institutions that rely on MSPs or run ScreenConnect internally should treat this as a supply-chain and third-party exposure as well as a patching task.

The practical response is to confirm the patched version is deployed, review recent sessions, and ask providers to confirm their own status.

What to do now

1. Confirm whether ScreenConnect is used internally or by your MSPs, and verify the patched version for CVE-2026-84869 is installed.
2. Ask each MSP in writing whether it has patched and whether it saw suspicious guest sessions.
3. Review recent ScreenConnect session logs for unexpected file transfers or executions on technician hosts.
4. Limit the privileges and network reach of technician workstations and monitor them with endpoint detection.
5. Record the issue in your third-party risk register and escalate any suspected compromise through your incident process.