SCKit Campaign Exploits Patched ScreenConnect Flaw, Raising MSP Risk



Blackpoint Cyber reports that the SCKit campaign against ConnectWise ScreenConnect exploits CVE-2026-84869 (CVSS 9.9), a patched critical flaw, not a new vulnerability.

- The ongoing campaign targets ConnectWise ScreenConnect deployments.
- It exploits CVE-2026-84869, rated CVSS 9.9, a critical flaw that has already been patched.
- Blackpoint Cyber's Adversary Pursuit Group recovered the attacker toolkit and shared details with The Hacker News.
- The activity is not based on a new vulnerability, which points to unpatched instances as the exposure.
- Remote support sessions could become attack paths into managed service provider environments.

What was reported

Blackpoint Cyber's Adversary Pursuit Group (APG) has described an ongoing campaign aimed at ConnectWise ScreenConnect, the remote access software widely used for support sessions. According to the report, the campaign relies on a toolkit the researchers recovered, referred to as SCKit.

The key clarification is that the campaign does not rely on a new vulnerability. The toolkit exploits CVE-2026-84869, a critical flaw with a CVSS score of 9.9 that has already been patched.

Why it matters

Because the flaw is patched, the exposure lies mainly in deployments that have not applied the fix. Remote support tools sit in a trusted position: they connect providers to customer environments. The report's framing suggests that support sessions could serve as a route into managed service provider (MSP) environments and, by extension, the organizations they serve.

The source excerpt does not provide further technical detail, such as affected versions, indicators of compromise or the scale of the activity, so those points should be confirmed with the vendor and the original research.

Practical view

Institutions that run ScreenConnect themselves, or that rely on providers who do, should treat this as a patch-verification and third-party assurance task rather than an emergency requiring new technology.

What to do now

1. Confirm whether ScreenConnect is used in your environment and verify that the patch for CVE-2026-84869 is applied.
2. Ask your MSPs and support vendors in writing whether they run ScreenConnect and have patched this flaw.
3. Review ScreenConnect access logs and session history for unexpected or unauthorized activity.
4. Restrict exposure of remote support servers and require strong authentication for technician access.
5. Include remote access tools in vulnerability management and third-party risk reviews under your NCA ECC and SAMA CSF programs.