ConnectWise: ScreenConnect attacks continue against unpatched on-premises systems



ConnectWise has finished its investigation into unauthorized access to partner ScreenConnect environments and advises running technician client 26.6.5 or later. Attacks on on-premises setups with certain third-party extensions enabled are still being reported.

- ConnectWise says it has completed its investigation into unauthorized access to partner ScreenConnect environments.
- Customers are advised to make sure the technician client runs version 26.6.5 or later.
- Activity against on-premises environments is still being reported.
- The reported activity involves environments where the identified third-party extensions remain enabled.
- The source headline links the ongoing attacks to SCKit targeting unpatched systems.

ConnectWise has said it completed its investigation into unauthorized access that targeted ScreenConnect environments belonging to its partners. As part of its guidance, the company recommends that customers confirm their technician client is running version 26.6.5 or later.

What is still happening

According to the report, ConnectWise continues to receive reports of further activity against on-premises ScreenConnect environments. The reports concern deployments where the identified third-party extensions remain enabled. The source headline also associates the continuing attacks with SCKit, which is described as targeting unpatched systems.

The excerpt available to us does not give further technical detail, such as the names of the extensions, vulnerability identifiers or the number of affected organizations, so we do not speculate on them.

Why it matters

Remote access and support tools give privileged reach into managed endpoints and servers. For regulated institutions that use ScreenConnect directly or through an IT service provider, an unpatched or exposed instance is a risk worth checking promptly, even if no incident has been observed.

Suggested approach

Confirm whether ScreenConnect is used anywhere in your environment, including by vendors and managed service providers. Compare installed versions with the vendor guidance, review which extensions are enabled, and read the original ConnectWise advisory for the full list of affected components before deciding on changes.

What to do now

1. Inventory all ScreenConnect instances, including those operated by vendors and managed service providers.
2. Verify the technician client is on version 26.6.5 or later and update where it is not.
3. Review which third-party extensions are enabled on on-premises servers and disable those you do not need, following ConnectWise guidance.
4. Check access and activity logs on ScreenConnect servers for unexpected sessions or changes.
5. Ask your service providers to confirm their ScreenConnect patch status in writing.