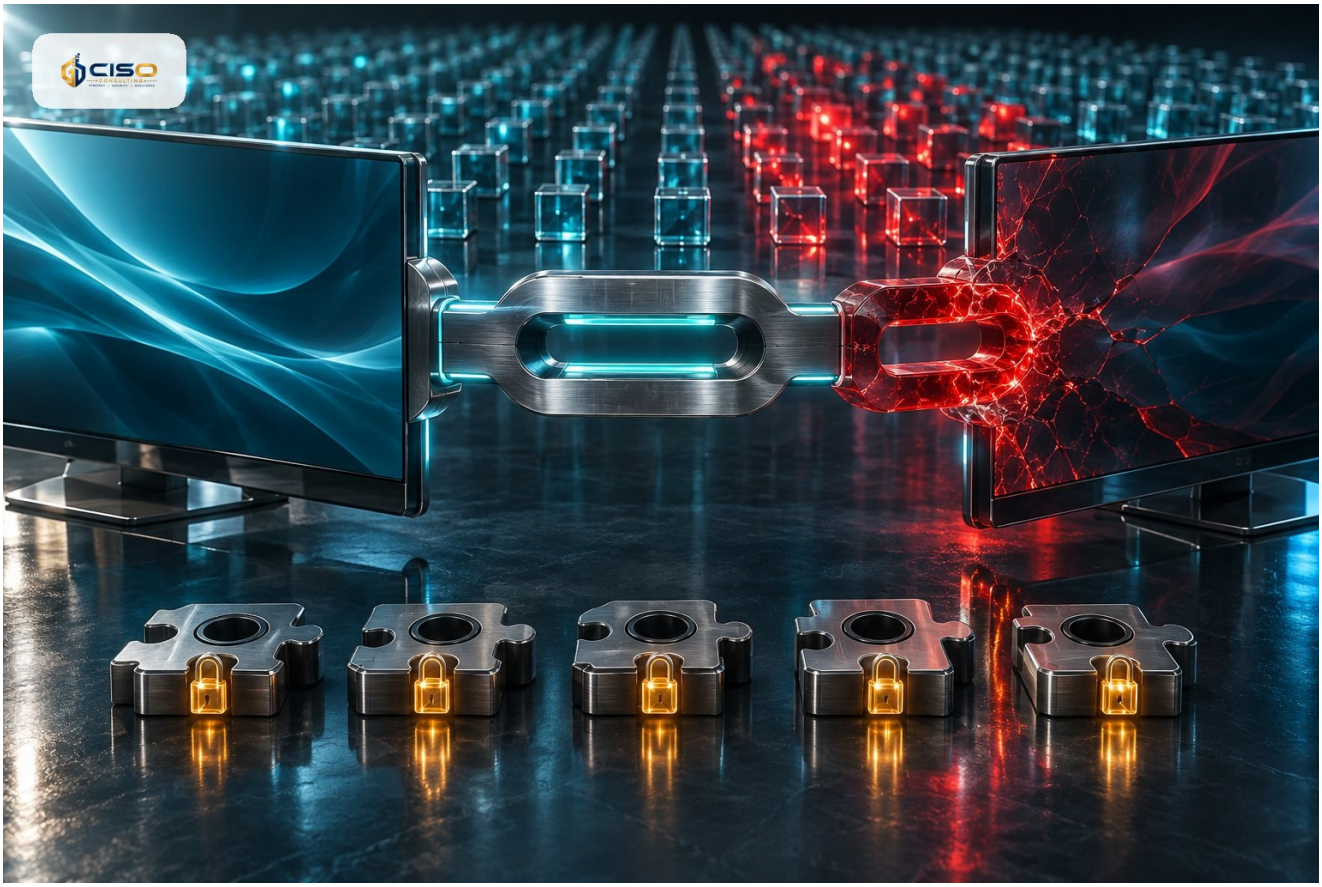
ScreenConnect Rogue Clients Found on 288 Endpoints; ConnectWise Disables Five Extensions



Attacks using rogue ScreenConnect clients reportedly reached at least 288 endpoints in 48 organizations. ConnectWise disabled five third-party extensions in partner environments after reports of unauthorized access.

- At least 288 endpoints across 48 organizations were targeted with rogue ScreenConnect clients.
- ConnectWise disabled five third-party extensions in partner environments as a precaution.
- ConnectWise states there is no evidence of a compromise of its infrastructure or of a vulnerability in ScreenConnect.
- The company's initial assessment is still preliminary, and the source excerpt does not give further technical detail.

ConnectWise has disabled five third-party extensions in partner environments following reports of unauthorized access involving ScreenConnect, its remote access tool. Reporting on the activity indicates that rogue ScreenConnect clients were used against at least 288 endpoints across 48 organizations.

What the vendor says

In an advisory on its site, ConnectWise stated that there is no evidence of a compromise of its own infrastructure or of a vulnerability in the ScreenConnect software. Its initial assessment is described as preliminary, and the available excerpt does not set out how the activity works or which extensions are affected.

Why it matters

Remote access tools are trusted by design, so an unauthorized client installed on an endpoint can look like normal administrative activity. Organizations that use ScreenConnect directly, or that rely on managed service providers who do, should confirm what is installed and who is permitted to connect.

Because the vendor has not pointed to a software flaw, patching alone may not address the exposure. The practical focus is on inventory, access control and monitoring of remote access tooling, together with a review of the ConnectWise advisory for updates.

What to do now

1. Inventory all ScreenConnect instances and clients, including those run by managed service providers, and remove any that are not approved.
2. Review the ConnectWise advisory and confirm whether any of the five disabled extensions were in use in your environment.
3. Hunt for unexpected remote access clients on endpoints and review recent remote session logs for unfamiliar connections.
4. Restrict remote access tool installation through application control and limit who can authorize connections.
5. Ask managed service providers to confirm their exposure and response in writing, in line with NCA ECC third-party requirements.