Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-84869: Critical ScreenConnect Client Flaw Under Active Exploitation

Date of Publication	Admiralty Code	TA Number
September 18, 2026	A1	TA2026273

Summary

First Seen: August 20, 2026
Malware: XMRig cryptominer
Affected Product: ConnectWise ScreenConnect client
Impact: ConnectWise ScreenConnect, a remote support and access platform widely used by MSPs and IT teams, is affected by a critical client-side vulnerability (CVE-2026-84869) in which missing authorization and improper privilege management in file-transfer handling allow a Guest in an active session to transfer and execute files on the Host without confirmation; servers are unaffected, but all clients prior to 26.6.5 are vulnerable and must be reinstalled or redeployed. Exploitation has been observed in an unattributed campaign since late August 2026, where socially engineered rogue clients executed a four-stage VBScript loader and backdoored clients pushed the same chain to every newly connected Host, producing worm-like spread. Payloads included a hidden ScreenConnect backdoor, UAC and Defender bypasses, a vulnerable WinRing0 driver, tunnelling and an XMRig miner, giving attackers persistent code execution on technician hosts and a pivot into downstream client networks.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-84869	ConnectWise ScreenConnect Improper Privilege Management and Missing Authorization Vulnerability	ConnectWise ScreenConnect	✓	✓	✓

Vulnerability Details

#1

ConnectWise ScreenConnect is a remote support and access platform used extensively by managed service providers and IT teams for remote assistance and unattended endpoint access. It is affected by a critical vulnerability tracked as CVE-2026-84869, arising from improper privilege management and missing authorization in the client's file-transfer handling during active Support and Access sessions. Under certain conditions, a Guest-side participant in an established session can transfer files to the Host and trigger their execution, including via elevated execution paths, without the authorization check or Host confirmation the product is designed to enforce. The weakness resides in the client and session-handling components; servers are not affected. All client builds prior to version 26.6.5 are vulnerable, and because the flaw is client-side, upgrading the server alone is insufficient, Host clients and Access agents must be reinstalled or redeployed afterwards.

#2

Exploitation activity consistent with the flaw has been observed in an unattributed campaign active since late August 2026. Initial access relied on social engineering rather than server compromise: tech-support scams abusing Quick Assist, a likely phishing-delivered installer, and a fake refund-form lure led victims to run rogue ScreenConnect clients pointing at attacker-controlled infrastructure. The clients spawned Windows Script Host to execute a four-stage VBScript loader that profiled the system, enumerated endpoint security products, checked available RAM as a likely virtual-machine test, and retrieved AES-encrypted payloads from cloud storage. Backdoored clients monitored for newly established Host connections and automatically queued the same script chain for transfer and execution with a Run action, producing worm-like propagation over legitimate support sessions and re-triggering on reconnection.

#3

Successful exploitation yields arbitrary code execution on the connecting Host. Depending on host profile, observed payloads delivered a user-level ScreenConnect backdoor; a UAC bypass with AMSI and Defender evasion and a concealed persistent client; or encrypted tunnelling, a vulnerable WinRing0 driver and an XMRig miner, with persistence via a WindowsServiceHost Run key and secondary RMM tools such as UltraViewer. For MSPs the impact is severe: an infected technician Host becomes a delivery mechanism into every downstream network it touches, and affected hosts should be reimaged rather than cleaned in place.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-84869	ConnectWise ScreenConnect client version before 26.6.5	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*:*:*	CWE-269, CWE-862

Recommendations

Upgrade All ScreenConnect Clients to 26.6.5 or Later Immediately: Version 26.6.5 contains the vendor fix and is the only complete remediation for CVE-2026-84869. On-premises servers must be running version 25.4 or later before they can move to 26.6.5, so operators on older branches should treat the intermediate upgrade as part of the same emergency change. Cloud instances receive the update automatically, but administrators must still refresh or remove and redeploy host clients and agents after the upgrade, otherwise stale client binaries remain vulnerable in the field.

Hunt for Exploitation Artefacts Before Declaring Systems Clean: Review ScreenConnect server audit logs for RunFiles or RanFiles entries executed from Process: Guest that reference 1.vbs through 4.vbs, WindowsServiceHost.vbs, or any Windows Script Host or PowerShell script, and treat any match as a confirmed compromise indicator. Inspect endpoints for ScreenConnect.WindowsClient.exe spawning wscript.exe, the WindowsServiceHost user Run key, the staging paths under %TEMP% and C:\Users\Public\Libraries\Default\Lib\Lib1, the malicious ScreenConnect instance ID 7a4d7d66502d4260, unauthorised RMM tools such as UltraViewer, and network connections to the infrastructure listed in the IoC table. Given the depth of the observed post-exploitation tooling, hosts showing this activity should be reimaged from known-good media rather than cleaned in place.

Apply Temporary Workarounds Where Patching Is Delayed: Remove or disable the TransferFiles permission, or TransferFilesInSession in legacy versions, from all roles to block in-session file transfer and remote execute features, which is the vendor's interim guidance from September 3. Enforce session policies that require explicit Host confirmation where the option exists, restrict elevated session modes, and use endpoint application control to prevent execution from user-writable paths and to constrain child processes spawned by ScreenConnect client binaries. These measures reduce exposure but do not remove the underlying flaw, so they must be paired with a committed upgrade date.

Run a Credential Hygiene Campaign: Because the flaw is exploited through sessions the system already trusts, reset administrator and privileged user passwords, enforce multi-factor authentication on all ScreenConnect accounts, and validate every user and agent account against an approved inventory to remove any account created or modified during the exposure window.

Reduce the Attack Surface of the ScreenConnect Deployment: Restrict web interface and relay access to trusted IP ranges with firewall rules or a reverse proxy, place ScreenConnect behind a VPN or on internal networks where the operating model allows, segregate ScreenConnect instances from sensitive network segments, enforce SSL/TLS, remove unused extensions and apply least privilege to all roles. Internet-exposed, unpatched instances are the population most likely to be hit next.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	
Execution	T1059: Command and Scripting Interpreter	T1059.005: Visual Basic
		T1059.001: PowerShell
	T1204: User Execution	T1204.002: Malicious File
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1219: Remote Access Software	
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1027: Obfuscated Files or Information	
	T1070: Indicator Removal	T1070.004: File Deletion

Tactic	Technique	Sub-technique
Defense Evasion	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
	T1564: Hide Artifacts	
Discovery	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1082: System Information Discovery	
Lateral Movement	T1570: Lateral Tool Transfer	
Command and Control	T1105: Ingress Tool Transfer	
	T1102: Web Service	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1572: Protocol Tunneling	
Impact	T1496: Resource Hijacking	T1496.001: Compute Hijacking

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	08bc4e82883eb42fc5219b206555b7a02a879860c76b4a12b2f82a64f6cc9020, de3b6836a88ae4b117e3b6de0e9cce3cd56a2b27b462d69e50c2fcac4089a457, 19a3534da9f60c726be426ec5cc2b72c2d1254fefa0782bd2f08ef08117f3260, 110fffc85370bb7cc60fa023447165c7e99175473d76bc5ffb2abecaa3a41d66, de89d560fc8302c778d88e3938327b240fa0db9a64fc1d5643067eedcbd2aede, ffd6d23f579571cc61936145791975da78b6ae914d780a9447a8f53c3688a0de
IPv4	45[.]13[.]237[.]190, 146[.]59[.]55[.]107, 45[.]32[.]192[.]150, 15[.]204[.]185[.]204
IPv4:Port	131[.]123[.]40[.]98[:]8041
Domains	tele-sync[.]opik[.]net, borertors92[.]anondns[.]net, homehub[.]opik[.]net
Filename	1.vbs, 2.vbs, 3.vbs, 4.vbs, WindowsServiceHost.vbs, WindowsServiceHost.bat, value.txt, map.txt, out.tmp, out.enc, user.enc, acc.enc, combo.enc, runner.ps1, PyTorchFix.ps1, Password.exe

TYPE	VALUE
Filename	sys_cache.zip, Themes.exe, SearchIndex.exe, svcdrv64.sys
File Path	%TEMP%\value.txt, %TEMP%\map.txt, %TEMP%\out.enc, %TEMP%\runner.ps1, %APPDATA%\Microsoft\Windows\Templates\Classic\sys_cache.zip, C:\Users\Public\Libraries\Default\Lib\Lib1
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run -> WindowsServiceHost
ScreenConnect Instance ID	7a4d7d66502d4260
Detection Name	Trojan:Script/Wacatac.H!ml

Patch Links

https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin

https://github.com/ConnectWise-Advisories/Disclosures/tree/main/CVE-2026-84869

References

https://www.connectwise.com/company/trust/security-bulletins/2026-09-08-screenconnect-bulletin

https://arcticwolf.com/resources/blog/cve-2026-84869/

https://www.huntress.com/blog/rogue-screenconnect-installations

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 18, 2026 • 04:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com