PUBLIC PREVIEW — FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Enterprise VPN Targeting Resurges. SonicWall Back at the Top.

SonicWall VPN targeting reversed course after a documented 92.9% decline, with coordinated credential attacks and management API scanning making SonicWall the most targeted single-vendor perimeter product this week at 72.2% of all enterprise VPN sessions. This session spike matches early warning indicators from GreyNoise Ten Days Before Zero research — a pattern that has preceded new SonicWall vulnerability disclosures by a median of 11 days. A coordinated VNC scanning campaign probed non-standard ports with per-target intensity far exceeding typical reconnaissance. Two independent infrastructure clusters converged on ConnectWise ScreenConnect and enterprise remote access products globally — without coordination.

2.5M+	72.2%	4.5M	2
SONICWALL SESSIONS ↑ AFTER 92.9% DECLINE	SONICWALL SHARE OF VPN TARGETING · 4 VENDORS HIT	VNC CAMPAIGN · FAR ABOVE TYPICAL INTENSITY	INDEPENDENT CLUSTERS · SAME CVE, DIFFERENT INFRASTRUCTURE

WHAT'S INSIDE

1 SonicWall VPN Targeting Resurges After 92.9% Decline

After weeks of documented decline, SonicWall is back as the dominant VPN target — API scanning and credential attacks hit simultaneously at a near 1:1 ratio, accounting for 72.2% of enterprise VPN-targeted activity. This resurgence exhibits multiple early warning indicators from the GreyNoise Ten Days Before Zero framework — patterns that have preceded new SonicWall disclosures by a median of 11 days (greynoise.io/resources/ten-days-before-zero).

2 VNC Scanning Campaign Probes Defender Blind Spot

A coordinated three-IP cluster probed non-standard VNC ports 5902–5910 with per-target intensity far exceeding typical scanning — targeting configurations that most organizations don't monitor. VNC receives less defensive attention than RDP or SSH, which is exactly why it's being targeted.

3 Two Independent Clusters Converge on ConnectWise ScreenConnect

A Netherlands-based cluster and an AWS-hosted platform independently target CVE-2024-1709 (CVSS 10.0) globally. Independent convergence on the same vulnerability — from separate infrastructure and tooling — signals ScreenConnect has become a consensus high-value target.

4 IoT Credential Pressure Remains Persistently Elevated

Default credential attacks continued at elevated baseline levels. Realtek CVE-2014-8361 remains the most broadly weaponized IoT vulnerability — integrated into 15 botnets with 6,219 malicious IPs active in the last ten days.

Want the full brief?

GreyNoise customers get complete IOCs, infrastructure attribution, and role-based recommendations every week.

greynoise.io/contact