PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Cisco and Fortinet VPN File-Read Attempts Rise About Sixfold. SonicWall and RDP Guessing Climb.

Adversaries stepped up file-read attempts on Cisco and Fortinet VPN appliances through two flaws known exploited since 2021. SonicWall VPN logins and Remote Desktop password guessing rose alongside.

About 6x
CISCO AND FORTINET VPN FILE-READ ATTEMPTS

About 1,500
MALICIOUS IPS A DAY AT THE CLOSE, FROM DOZENS

5.9x
SONICWALL SSL VPN LOGIN ATTEMPTS

59%
RDP PASSWORD ATTEMPTS FROM THREE HOSTING IPS

WHAT'S INSIDE

1 Cisco and Fortinet VPN file-read attempts rise about sixfold

Malicious IPs attempting Cisco ASA CVE-2020-3452 and FortiOS CVE-2018-13379 went from dozens a day to about fifteen hundred. Neither flaw needs a login, and both have been known exploited since 2021.

2 A PHP framework flaw rose alongside them

Daily IPs on ThinkPHP CVE-2022-47945 rose on the same days by similar amounts as the two VPN flaws. Three unrelated products moving as one very likely points to a single toolset.

3 SonicWall VPN logins rise nearly sixfold

SonicWall SSL VPN login attempts rose 5.9 times and SonicOS API probes 11.8 times. Overflow attempts on two SonicOS flaws rose in bursts on the same days as the Cisco and Fortinet rise.

4 Three hosts double Remote Desktop guessing

Three hosting IPs sent 59% of RDP Bruteforce Attempt traffic, and without them volume was flat. Two went quiet mid-period and one was new, so address blocks lapse within days.

Want the full brief?

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

greynoise.io/contact

© 2026 GreyNoise, Inc.