PUBLIC PREVIEW: FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

This Week: Early-Warning Spikes on Enterprise Edge and VPN Devices.

Late in the week, GreyNoise's early-warning detection flagged validated spikes against FortiOS SSL VPN, Cisco SSL VPN, Ivanti EPMM, and NETGEAR devices; elevations of this kind have historically preceded new vendor vulnerability disclosures. Beneath them, a single host ran file-inclusion exploitation and coordinated /24 blocks brute-forced RouterOS and RDP for credentials, almost all on short-lived rented hosting. The durable signal was behavioral: shared client fingerprints and hosting blocks, not rotating IP addresses.

84%	~298x	9 hosts	Behavioral
ONE /24 = SHARE OF ROUTEROS BRUTE-FORCE	FORTIOS SSL VPN EARLY-WARNING SPIKE VS A NORMAL DAY	ONE /24 RUNNING RDP IN LOCKSTEP	THE DURABLE SIGNAL, NOT IP ADDRESSES

WHAT'S INSIDE

1 Early-warning spikes on enterprise edge and VPN devices

GreyNoise's early-warning detection flagged validated late-week spikes against FortiOS SSL VPN (CVE-2018-13379, a CISA KEV), Cisco SSL VPN, Ivanti EPMM, and NETGEAR. Elevations of this kind have historically preceded new vulnerability disclosures or renewed exploitation affecting the same vendor. Confirm patch status and reduce exposure on these devices now.

2 A single source ran a file-inclusion exploit chain

One DIGI VPS host (103.168.66.158) generated high exploitation volume, running Generic Path Traversal at scale alongside ThinkPHP (CVE-2022-47945, CVSS 9.8), Joomla, and Linear eMerge file-inclusion exploits, a direct route to code execution. Tracking routes to code execution is often more valuable than tracking individual CVEs, because attackers frequently chain multiple weaknesses together to reach RCE.

3 RouterOS API brute-force from a single /24

Two VPSVAULT hosts on 45.198.224.0/24 ran roughly 665,000 RouterOS Bruteforcer attempts against the MikroTik management API on TCP/8728, about 84 percent of that activity corpus-wide. No CVE is involved; this is pure valid-credential discovery against a control surface often left internet-facing.

4 A coordinated nine-host RDP fleet on one /24

Nine hosts on 91.238.181.0/24 (FBW NETWORKS) ran coordinated RDP scanning and brute-force in lockstep; the lead host alone targeted United States and Canada. The coordination signal is the shared /24 and uniform behavior, not a fingerprint, and the dense, evenly-loaded /24 is consistent with initial-access preparation.

Want the full brief?

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

greynoise.io/contact