PUBLIC PREVIEW, FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

Amid FortiBleed, GreyNoise Tracks the Fortinet Attack Surface, as Cisco VPN Brute-Force Sources Surge

GreyNoise is not attributing this activity to FortiBleed; the brute-force it tracked stood down in early June. Also this week: a German-hosted source harvesting application secrets, and broadening Hikvision camera targeting.

Fortinet
GREYNOISE'S READ ON THE SSL VPN BRUTE-FORCE SURFACE, WHICH STOOD DOWN IN EARLY JUNE

3,645
SOURCES BRUTE-FORCING CISCO SSL VPN ON JUNE 23, UP FROM DOUBLE DIGITS A WEEK EARLIER

Secrets
A GERMAN-HOSTED SOURCE HARVESTING LARAVEL AND TELEMESSAGE CREDENTIALS

Hikvision
CAMERA RCE TARGETING BROADENED ACROSS NEW AND RETURNING SOURCES (CISA KEV)

WHAT'S INSIDE

1 GreyNoise's read amid FortiBleed

Amid FortiBleed, GreyNoise is providing telemetry on the same Fortinet surfaces the reporting names, without attributing the activity at this time. A Fortinet SSL VPN brute-force GreyNoise tracked for months stood down in early June, and exploitation of the named vulnerabilities is minimal. Reset Fortinet credentials and enforce MFA per CISA guidance.

2 Cisco SSL VPN brute-force sources surge

Distinct sources brute-forcing Cisco SSL VPN portals jumped to 3,645 on June 23, from double digits a week earlier. A subset also hit other vendors' VPN logins, so MFA and account lockout belong on every VPN edge, not just Cisco.

3 Secrets-theft source hunts Laravel and TeleMessage credentials

A German-hosted source is harvesting application secrets, probing Laravel CVE-2024-29291 and TeleMessage CVE-2025-48927 (/heapdump, CISA KEV) alongside heavy scanning for exposed .env, Git, AWS, and Spring Boot Actuator files. The focus points to deliberate harvesting, not opportunistic crawling.

4 Hikvision camera targeting broadened

Scanning for the Hikvision /SDK/webLanguage endpoint (CVE-2021-36260, CISA KEV) broadened across new and returning Netherlands-hosted sources. Treat any exposed Hikvision device answering these probes as potentially vulnerable.

Want the full brief?

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

greynoise.io/contact