GREYNOISE Intelligence

Event Date: 25 September 2025
Report Date: 29 September 2025

TLP: CLEAR

Executive Situation Report | Reconnaissance Surge on Cisco ASA Preceded Zero-Days

Key Judgments & Evidence

1. **Surges in Cisco ASA scanning are correlated with future vulnerability disclosures, including the Cisco zero-days disclosed on 25 September.**
   - GreyNoise observed ~25,000 IPs scanning Cisco ASA in late Aug–early Sept, a clear spike over baseline.
   - Cisco disclosed CVE-2025-20333 (CVSS 9.9) and CVE-2025-20362 (CVSS 6.5) on 25 Sept.
   - GreyNoise observed a similar occurrence in April 2025, where a surge in ASA scanning preceded the disclosure of CVE-2025-32433.
2. **State-sponsored threat actors are actively exploiting these zero-days, presenting critical risks to governments and enterprise networks.**
   - ASA/FTD are widely deployed at the perimeter across government and private sectors.
   - Standard EDR defenses do not protect against attacks.
   - Cisco assesses ArcaneDoor actors are exploiting these flaws; UK NCSC confirmed malware on Cisco devices.
   - CISA issued ED 25-03 requiring fixes within 24 hours and added both CVEs to KEV.
3. **Successful exploitation gives attackers complete control of affected devices and long-term access to sensitive information.**
   - CVE-2025-20333 allows root RCE with credentials; CVE-2025-20362 allows unauthenticated WebVPN access; both have been chained in exploitation.
4. **Organizations should broaden defensive scope to include brute-force attacks against Cisco SSL VPNs.**
   - GreyNoise observed Cisco SSL VPN brute-force attempts resume 25 Sept from a single client fingerprint.

Source Countries:
BRAZIL (64%)
ARGENTINA (8%)
UNITED STATES (8%)

Target Countries:
UNITED STATES (97%)
UNITED KINGDOM (5%)
GERMANY (3%)

**Source and target information based on observations from the past 90 days since initial 4 Sept reporting*
**Percentages can exceed 100% as threat actor IPs may target multiple countries*

Strategic Threat Context

ESPIONAGE:

ArcaneDoor actors have been reported exploiting Cisco ASA/FTD zero-days to infiltrate government networks.

RANSOMWARE:

Ransomware groups have historically targeted Cisco ASA appliances for initial access and lateral movement.

GLOBAL IMPACT:

Past ASA vulnerabilities (e.g., CVE-2020-3452) were exploited worldwide within days of disclosure.

Recommended Actions

> Identify and patch all Cisco ASA/FTD devices affected by CVE-2025-20333 and CVE-2025-20362.

> Follow CISA ED 25-03: capture and submit forensic memory dumps, and isolate suspected compromised devices.

Implications

> Patching may not remove persistence; reimaging and credential rotation may be required.

> VPNs and firewalls tend to be high-value targets, with new zero-days likely to be exploited quickly.

> ED 25-03 imposes heavy forensic and remediation demands on large Cisco deployments.

Threat Actor Activity (Past 90 Days)

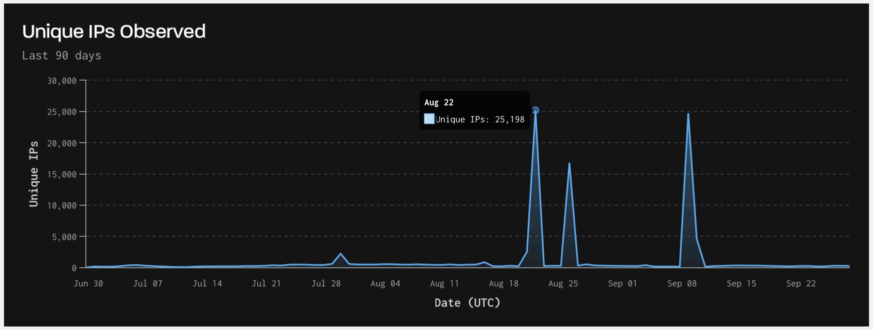

Figure 1. Cisco ASA Scanner activity (Source: GreyNoise Global Observation Grid (GOG))

Peak Activity:
25,198 unique IPs (22 August 2025)

Baseline: ~500 IPs daily

Percentage Increase: ~5,000%

Significant spike in threat actor IPs scanning for Cisco ASA devices.

__Data from:__ GreyNoise "Cisco ASA Scanner" Tag
Cisco ASA Appliance Software & Cisco Telnet/SSH Profiles

***Timeframe:** 22/26 Aug & 9 Sept 2025 Scanning Surge*
25 September 2025 Zero-Day Disclosures
***Source:** GreyNoise Intelligence*

Original GreyNoise Analysis