PUBLIC PREVIEW | FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

The Exposure Inventory Is the Weak Link

Every finding this period lands on an asset organizations expose to the internet deliberately and do not fully inventory: a gateway appliance owned by another team, a legacy application server, a relocated service, and a forward proxy with no identified owner. Adversaries attempted to exploit CISA KEV-listed flaws across five remote access and gateway vendors. Ten rented hosts each swept a disjoint contiguous band, together tiling the low and high ends of the TCP port range, and ninety-two more ran a matched toolkit that tests whether a discovered proxy forwards traffic.

5 vendors
REMOTE ACCESS AND GATEWAY VENDORS ADVERSARIES TRIED TO EXPLOIT

17
COLDFUSION TAGS, 2009 TO 2026

~5 days
FOR 10 HOSTS TO SWEEP THEIR DISJOINT PORT BANDS

82%
OF ALL OPEN PROXY SCANNER AND SOCKS5 PROXY SCANNER PROBES, FROM 92 HOSTS

WHAT'S INSIDE

1 Five vendors, all nine flaws already KEV-listed

Adversaries attempted to exploit KEV-listed flaws across Ivanti, Palo Alto Networks, Citrix, F5 and Fortinet, several listed months ago. Ordering this work by observed volume runs backwards: adversaries made double-digit attempts against the maximum severity flaw while scanning the same product classes hundreds of thousands of times. Rank by KEV listing and reachability instead.

2 Seventeen ColdFusion tags, one likely module list

Adversaries attempted to exploit Adobe ColdFusion across seventeen distinct GreyNoise tags in one window, spanning 2009 to 2026 and including a maximum severity path traversal added to the KEV catalog in July. No single tag dominates the distribution, which is consistent with one module list run against every instance a source finds.

3 Ten hosts split the low and high ends of the port range

Ten rented hosts each took a disjoint contiguous band of the TCP port range, together covering its low and high ends. GreyNoise observed none of them before 12 August, and all ten presented a single TCP client fingerprint. They enumerated a service relocated to a port inside those bands on the same schedule as one sitting on its default.

4 Ninety-two hosts test whether a proxy really forwards

Two hosting networks ran a matched toolkit against unauthenticated web proxies and SOCKS5 relays, producing 82% of the Open Proxy Scanner and SOCKS5 Proxy Scanner probes GreyNoise observed this period. The two scanners ran within 1% of each other on both networks, on separate connections rather than one probe tripping two tags. Audit each proxy you operate from an external address and confirm the service refuses the relay.

Want the full brief?

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

greynoise.io/contact