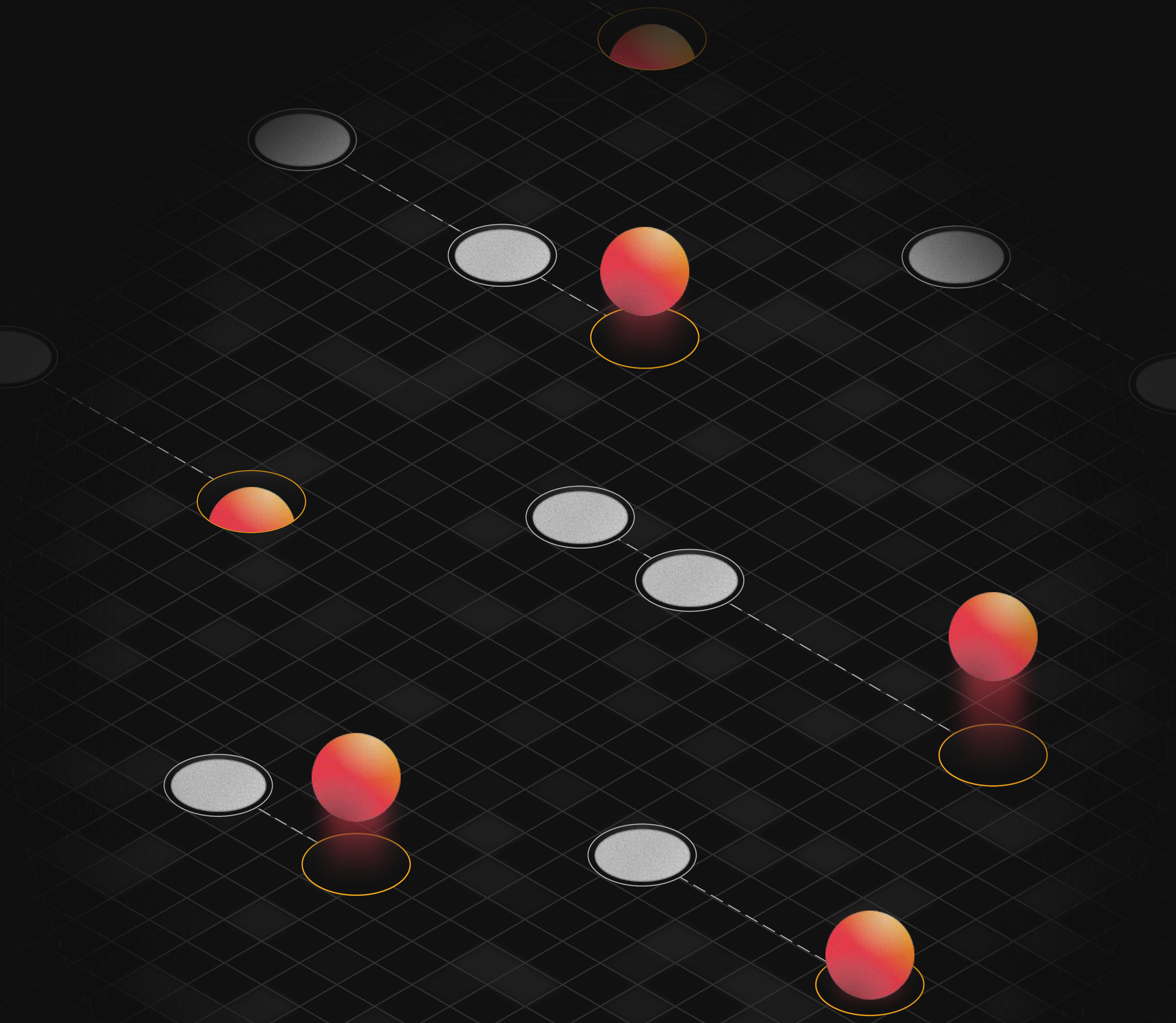
GREYNOISE



Early Warning Signals: When Attacker Behavior Precedes New Vulnerabilities

An empirical analysis of pre-disclosure spikes in malicious activity — and what they signal about the vulnerability lifecycle.

Contents

Key Takeaways

This report explores the correlation between spikes in attacker activity and subsequent CVE disclosures in edge technologies. Our findings suggest a repeatable pattern with predictive value — useful for all defenders, from analysts to CISOs.

1 Spikes in attacker activity often precede new cyber vulnerabilities.

In 80 percent of cases we analyzed, significant spikes in opportunistic attacker activity against edge technologies were followed by the disclosure of a new CVE affecting the same technology within six weeks. This recurring pattern may offer early warning value.

2 These spikes give defenders a defined window to prepare.

The clustering of new CVEs within six weeks of attacker spikes provides defenders with a concrete timeframe to increase monitoring, harden systems, and preemptively act — even before a vulnerability is known. CISOs can use this window to justify early planning or investment.

3 Blocking early reconnaissance may keep systems off attacker inventories.

Spikes may reflect exploit-based reconnaissance designed to identify exposed systems. Blocking the associated IPs during these phases may prevent inclusion in attacker inventories — reducing the likelihood of being targeted later, even if different IPs are used for exploitation of the new CVE emerging weeks later.

4 Enterprise edge technologies show the strongest patterns.

After filtering out ambiguous cases and noise, all spike-CVE pairs we observed involved internet-facing assets commonly deployed in enterprise environments — such as VPNs, firewalls, and products from vendors like Cisco, Fortinet, Citrix, and Ivanti.

5 Most spikes involved real exploits — not scanning.

The majority of activity leading up to CVEs was not generic scanning but exploit attempts against previously known vulnerabilities. This supports two likely motives: testing inputs that may lead to new CVE discovery, or inventorying systems for future exploitation when a new flaw becomes known.

6 State-sponsored actors have repeatedly targeted edge infrastructure.

Nation-state groups like the Typhoons have reportedly focused on enterprise-focused edge devices for pre-positioning, surveillance, and access persistence. All products studied in this analysis are enterprise-focused edge systems, highlighting both enterprise and national security stakes.

Do Spikes in Attacker Activity Foreshadow New Vulnerabilities?

GreyNoise has repeatedly observed spikes in attacker activity — including scanning, brute forcing, and exploitation attempts — targeting specific technologies in the weeks leading up to the public disclosure of new vulnerabilities affecting those same technologies.

This raised a compelling hypothesis:

> *Could these individual incidents reflect a broader trend — one where attacker behavior, as measured by GreyNoise's Global Observation Grid (GOG), offers an early warning signal for the emergence of new CVEs?*

The data supports this possibility. After analyzing all GreyNoise tags (CVSS 6+ CVEs) associated with edge technologies, **we found a consistent pattern: spikes in attacker activity often precede new vulnerability disclosures.** This pattern was only observed across a specific subset of enterprise edge products — spanning eight vendors — though we did not limit our analysis to enterprise technologies.

This report offers defenders — from analysts to CISOs — a new source of actionable intelligence to improve readiness and reduce exposure ahead of new vulnerabilities being announced.

Codifying the Relationship

To test our hypothesis, we analyzed attacker activity over time — specifically, the daily count of unique IPs observed — across GreyNoise tags associated with edge technologies. These included tags tracking scanners, crawlers, and brute forcing, as well as tags linked to CVEs with a CVSS score of six or higher. Our analysis began in September 2024, following a major enhancement of GreyNoise's Global Observation Grid (GOG).

We used the same set of edge-focused tags featured in our prior report on resurgent vulnerabilities. Our goal this time: to identify statistically significant spikes in malicious activity and examine whether they consistently preceded the disclosure of new CVEs, helping us assess whether attacker behavior could serve as a signal for defenders.

Defining a Spike

To ensure rigor, we only counted a day's activity as a "spike" if it met two conditions:

1. **Globally Elevated:**
   The daily unique IP count exceeded the median for that tag's entire history, plus two times the interquartile range (IQR).

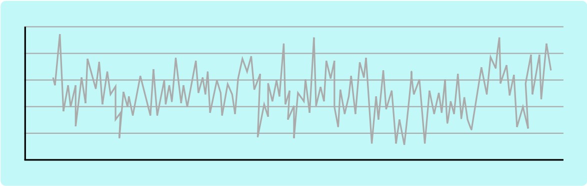
2. **Locally Elevated:**
   The daily count also exceeded the 28-day rolling mean (14 days before and after), plus two rolling standard deviations (same period as rolling mean).

This dual threshold helps ensure the spike is both globally anomalous and locally unusual — filtering out noise and highlighting activity that truly stands out.

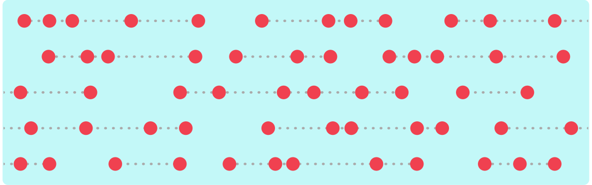
Narrowing the Dataset to Maximize Signal Integrity

To ensure the integrity of our findings, we filtered out tags that introduced noise or lacked meaningful trend signals. Specifically, we excluded tags that exhibited:

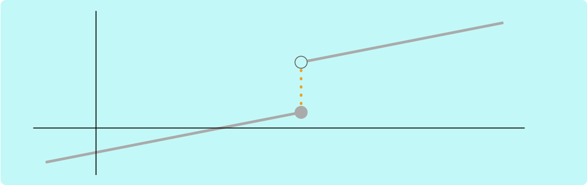
- **Quasi-stationarity:** Consistent, heartbeat-like patterns that lacked clear anomalies.



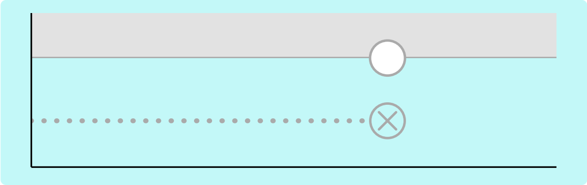
- **Excessive CVE volume:** Vendors with so many vulnerabilities that linking specific spikes to individual CVEs became statistically meaningless.



- **Discontinuous data:** Gaps or irregularities in the time series that made trend analysis unreliable.



- **No qualifying spikes:** Tags that did not meet our defined threshold for anomalous activity.



After applying these filters, we were left with 216 statistically significant spikes in attacker activity, observed from September 2024 onward. Each spike was then paired with the next newly disclosed CVE affecting the same product associated with the tag.

Notably, the resulting set of matched pairs exclusively involved edge technologies from eight enterprise vendors — even though we did not limit our initial dataset to enterprise products. This pattern emerged organically through the data.

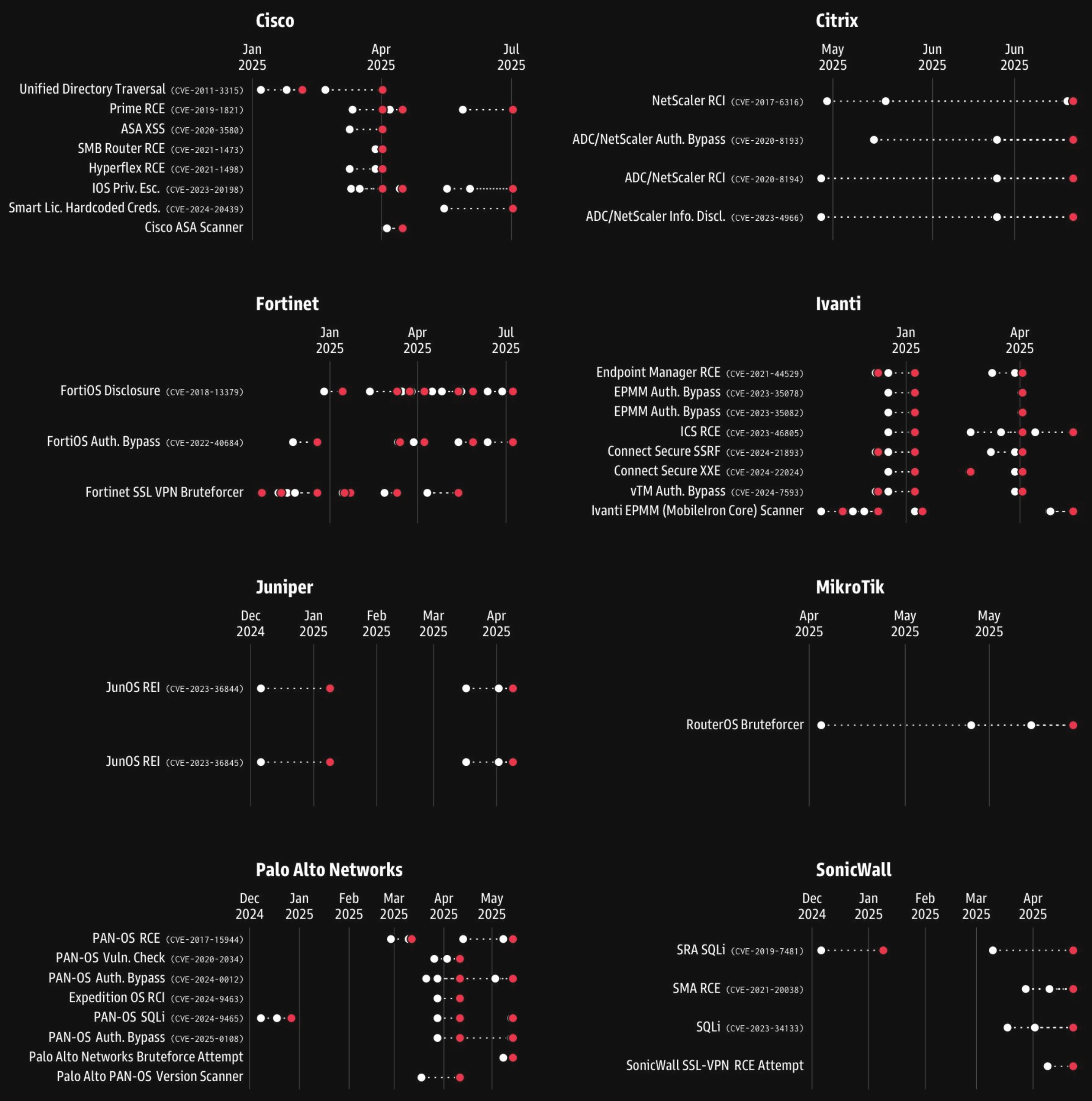
Revealing the Signal: Attacker Activity as a Leading Indicator of New Cyber Vulnerabilities

Across eight enterprise vendors, GreyNoise observed that spikes in attacker activity (white dots) against specific edge technologies often preceded the disclosure of new CVEs (red dots) affecting those same products — typically within six weeks. While not necessarily causal, this recurring pattern suggests that attacker behavior can serve as an early signal for emerging vulnerabilities, especially in perimeter-facing systems.

The chart below highlights only those spikes that were followed by a CVE disclosure within six weeks.

Hidden Signals Before The Storm

Each **white** dot represents a confirmed spike event on that GreyNoise tag. Each red dot represents a new published CVE.



Note free X-axis scales

MikroTik, for example, has a signal but probably shouldn't be used to inform preemptive defenses. With several spikes before the one emergent CVE, it's difficult to draw any correlation between the spikes and the new CVE. Citrix follows a similar pattern, albeit less pronounced.

On the other hand, other vendors tend to have clear and definitive patterns. Ivanti is perhaps the most striking example, with very tight and marked spike-to-new-CVE patterns. Likewise, Fortinet is an example of very rapid successions of 'there's a spike' and 'there's a new CVE.' In these situations, **defenders sometimes have days to prepare before a new CVE emerges.**

Attackers Leveraging Old Vulnerabilities

The age of each vulnerability also stood out to us. Take Cisco CVE-2011-3315, for example — we observed significant spikes in activity against this 14 year old vulnerability just before the emergence of a new vulnerability. Or CVE-2017-15944, affecting PAN-OS — an eight year old flaw still in play, serving as an indicator of new vulnerabilities affecting PAN-OS.

This theme is like a beating drum in our recent research: **old vulnerabilities are persistent problems, and attackers know how to use them to inflict damage and reap the rewards of successful operations.** In our last report, we stressed the importance of monitoring resurgent exploitation against old, forgotten vulnerabilities. Once again, intelligence in this report suggests old vulnerabilities remain among the most salient of topics.

Why Might Attackers Do This?

Several plausible motivations may explain why attacker behavior often spikes ahead of new vulnerability disclosures — and why defenders should take notice:

1. **Target confusion through broad activity.**

   For vendors like Ivanti, we frequently observed simultaneous spikes across multiple tags. This may be an intentional tactic to obscure the attacker's true focus. By triggering activity on several products, attackers could mislead defenders into thinking traffic is broad and opportunistic — when in fact it's concentrated and strategic.

2. **Pre-positioning through system inventorying.**

   Many spikes may reflect reconnaissance — attackers proving systems using older exploits to catalog exposed assets. These systems may later be targeted when a new vulnerability emerges. Even fully patched systems can be inventoried for future exploitation. Blocking IPs during this phase may prevent inclusion in these attacker inventories.

3. **Spikes as signals of zero-day discovery.**

   In some cases, spikes may reflect more than reconnaissance — they could represent active attempts to discover new vulnerabilities. This could explain the close timing between spike activity and subsequent CVE disclosures.

In all cases, defenders should view significant spikes in activity — especially across enterprise edge technologies — as potential signals of heightened attacker intent, whether for future exploitation or vulnerability discovery.

Defenders' Six-Week Critical Window

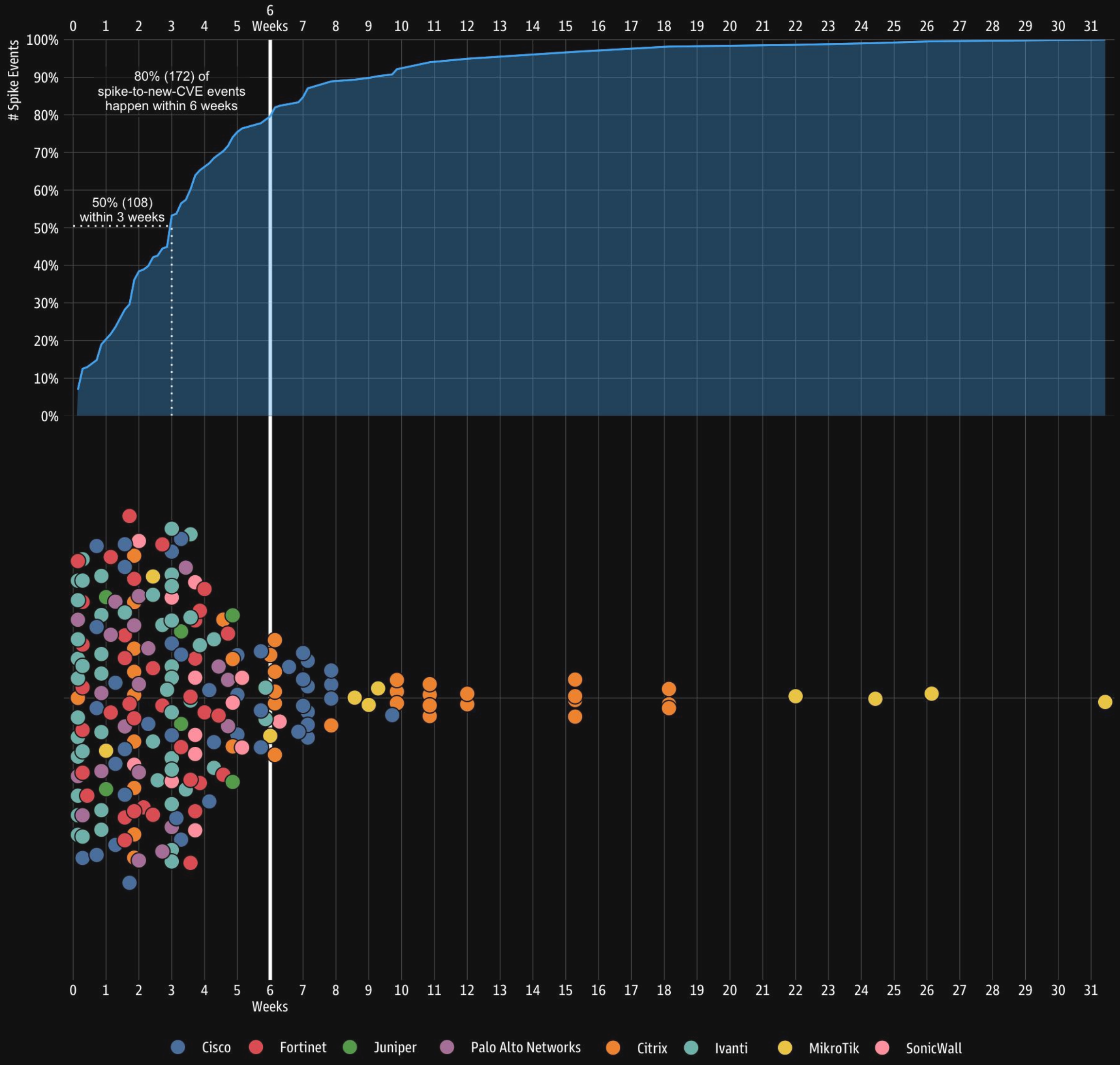
While the previous chart only visualized spike events where a new CVE followed within six weeks, the chart below expands the scope to all 216 spikes observed in our dataset. It reveals a consistent and useful trend:

> *Across all 216 spike events we studied, **50 percent were followed by a new CVE within three weeks, and 80 percent within six weeks.***

This finding holds strong across the enterprise edge technologies we examined — offering defenders a reliable, actionable window to prepare. Whether that means adjusting patching readiness, launching focused threat hunts, or escalating internal discussions about resource allocation, this pattern can serve as an early planning marker.

Spike-To-New CVE Delta Distribution

Each dot is a confirmed GreyNoise tag spike. Position on X axis is the delta between tag spike and a new CVE being published by the vendor associated with the tag.



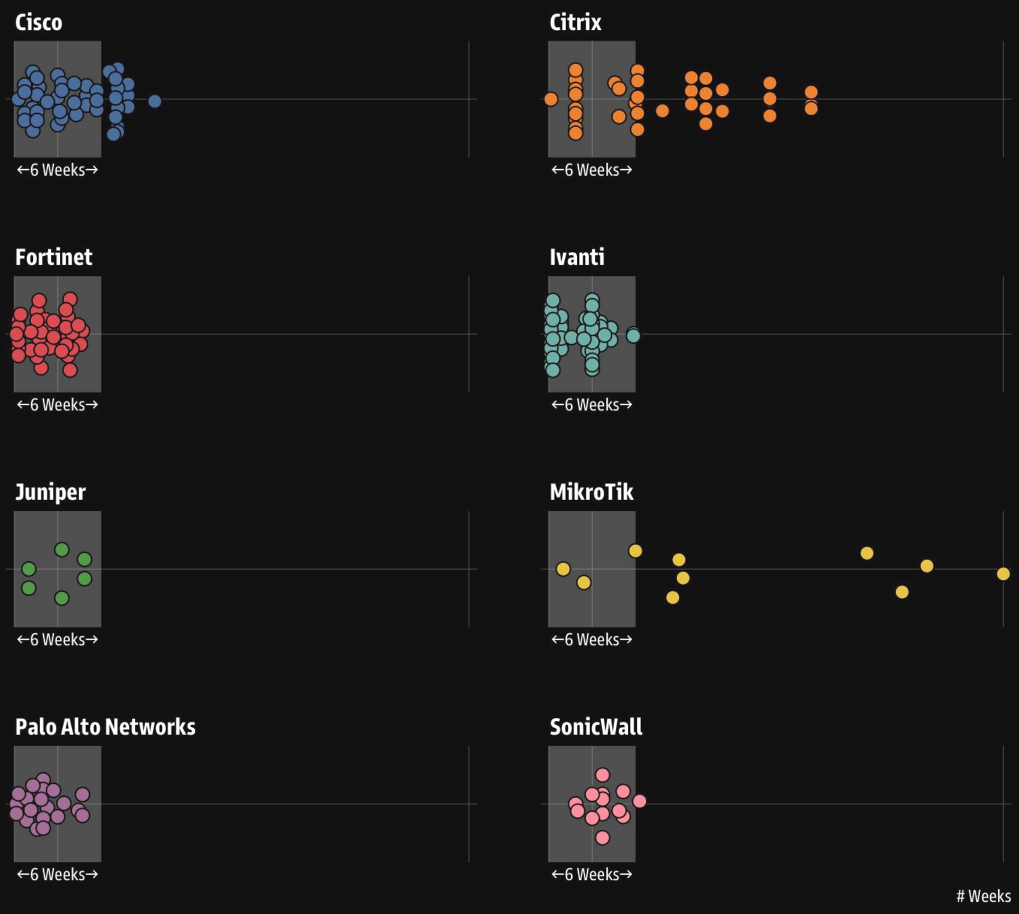
That said, this is not a universal rule. The trend was observed only in a narrow set of enterprise-focused edge products, and future attacker behavior may differ. While the six-week window offers a powerful early signal, defenders should remain vigilant long after it passes.

Why the Skew?

The six-week window doesn't apply evenly across all vendors. As seen below, the pattern breaks down most notably for Citrix, Cisco, and MikroTik — the primary drivers of outlier behavior in our dataset. Without them, nearly all the spikes would be followed by a new CVE within six weeks.

Tag Spike-to-CVE Delta Correlations By Vendor

The zero-to-six weeks spike-to-new-CVE correlation doesn't hold across all edge vendor technologies or GreyNoise tags, but is strong enough for organizations to use as an early warning system for many.



So while the six-week window is a useful planning marker for many products, it does not hold for all. Specifically:

Cisco:

Somewhat more consistent than Citrix, but still exhibits many long-tail cases beyond six weeks.

Citrix:

In about half of all spike cases, a new CVE follows more than six weeks later.

MikroTik:

Wide variability; attacker spikes are not a reliable signal for anticipating new CVEs.

Why Does This Signal Really Matter?

All of the spikes we analyzed occurred in enterprise-focused edge technologies — a category that continues to attract attention from sophisticated threat actors. State-sponsored groups have reportedly targeted edge infrastructure to gain footholds and establish persistence. **That makes this trend more than a statistical observation; it's a national security concern.** Our hope is that defenders can use the insights in this report to proactively identify and respond to emerging cyber threats.

Recommendations for Defenders

This report highlights a powerful signal: spikes in attacker activity often precede new CVEs. This gives defenders a rare chance to act early — before vulnerabilities are even disclosed. Whether you're a frontline analyst or a CISO, here are three ways to operationalize that signal:

1 Block Pre-Disclosure Activity to Stay Off Target Lists

Block IPs involved in significant spikes of exploit-driven reconnaissance. This can prevent your systems from being inventoried or fingerprinted before a new vulnerability is disclosed — making them less likely to be targeted once exploitation of that new CVE begins.

2 Don't Assume "Fully Patched" Means "Fully Safe"

Spikes may reflect reconnaissance that leads to new discoveries – not just attempts to exploit known flaws. Even patched systems might be probed in advance of a new CVE. Observing these spikes can inform early action or justify reallocation or defensive resources.

3 Use Spike-CVE Patterns for Strategic Planning

These patterns offer a practical planning window — often less than six weeks — between attacker activity and vulnerability disclosure. Use them to prioritize patching, strengthen visibility, harden exposed services, or reassess use of high-risk technologies.

> *If defenders leave with one takeaway, it's that attacker activity appears to not just react to vulnerabilities — it often precedes them. This finding challenges conventional reactive security models and introduces a new class of preemptive threat intelligence.*

Methodology

We analyzed attacker activity using GreyNoise's Global Observation Grid (GOG), focusing on edge technology tags from September 2024 onward — the point at which GOG coverage expanded significantly.

Spike Detection

A spike was defined as a statistically significant increase in daily unique IPs for a given tag.
A day qualified as a spike only if it met both of the following conditions:

Global Spike

Per tag over the full period, a day t was considered a global spike if:

$$x_t > \text{median}(x) + 2 \times \text{IQR}(x)$$

Where:

- x_t is the unique IP count for day t.
- x is the vector of daily unique IPs for that tag across all days.
- IQR is the interquartile range of x.

Local Spike

We also applied a local spike test, which considers short-term anomalies using a rolling window of 14 days before and after day t, excluding t itself (total: 28 days). A local spike was defined as:

$$x_t > \mu_{(t-14,\ t+14)} + 2\sigma_{(t-14,\ t+14)}$$

Where:

- μ is the rolling mean.
- σ is the rolling standard deviation.

Defining Spike-to-CVE Pairs

A tag day was labeled a spike only if it passed both tests. From there, we:

- Matched each spike to the first new CVE (CVSS 6+) affecting the same vendor/technology.
- Ensured each spike was linked to only one CVE, and each CVE could have multiple spikes associated.
- Filtered out vendors with quasi-stationary (heartbeat) activity, excessive CVE volume (noisy data), or discontinuous time series.

This process yielded 216 spike-CVE pairs across eight enterprise edge vendors, which became the basis of our findings.

GREYNOISE

Schedule a demo

Discover how GreyNoise can help you improve your SOC capacity, prioritize the most urgent vulnerabilities, and find emerging threats

greynoise.io/contact/sales