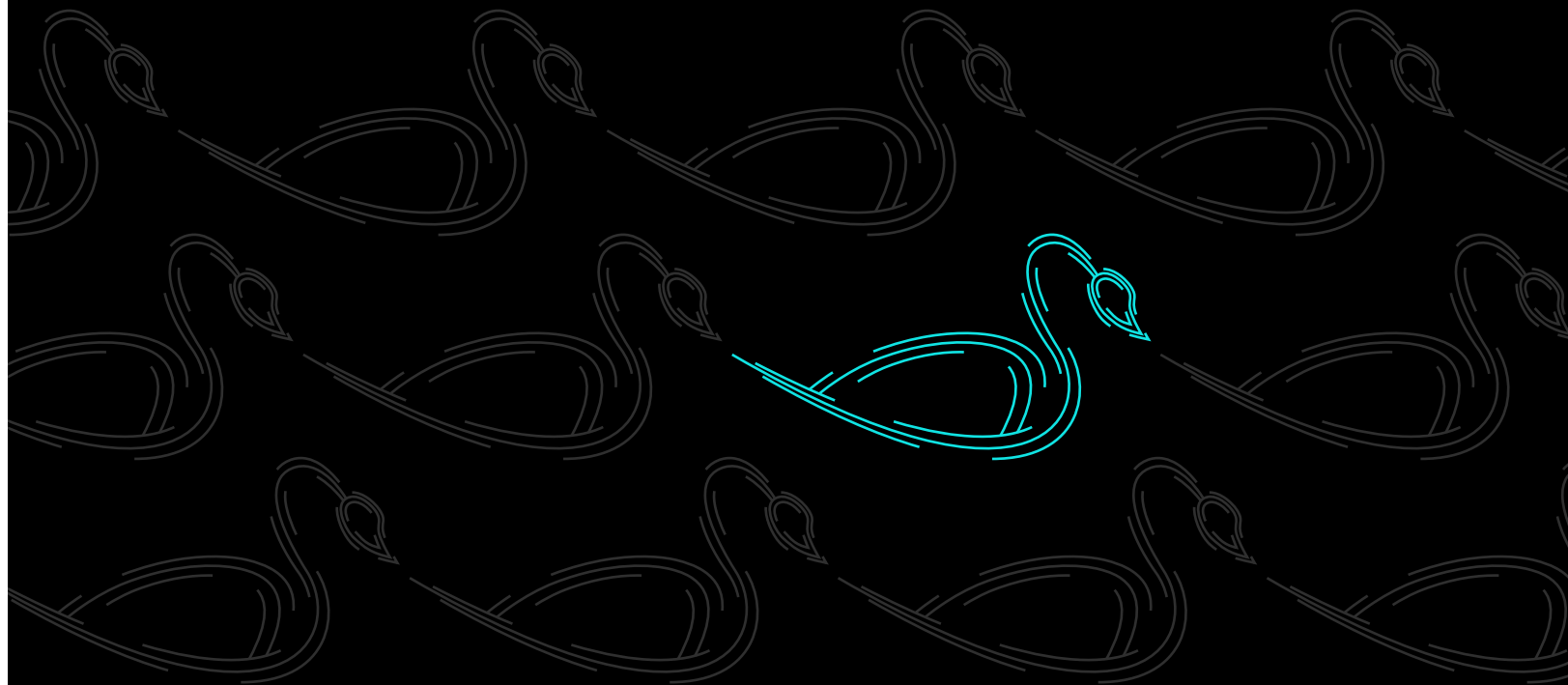


GREYNOISE

# A Blindspot in Cyber Defense

How Resurgent Vulnerabilities  
Jeopardize Organizational Security



From loud waves to quiet revivals,  
attackers around the world are exploiting  
resurgent flaws in critical systems.

# Table of Contents

---

Key Takeaways	3
---------------	---

---

The Strategic Risk of Resurgent Vulnerabilities: How Dormant Threats Complicate Cyber Defense	5
---	---

---

Defining Resurgent Vulnerabilities: A Behavioral Taxonomy	6
Eternal (Non-Resurgent)	6
Utility (Resurgent)	6
Periodic (Resurgent)	7
Black Swan (Resurgent)	7
Resurgence from a Different Perspective	10

---

A Critical Link: The Edge Connection	14
Resurgent Vulnerabilities Skew Toward High-Severity	15
Black Swan Vulnerabilities: The Most Router-Heavy Resurgent Category	16
A Security Blindspot: Attackers Exploit Small Business Gear	17

---

Resurgence Demands a Rethink of Patch Management	19
--	----

---

What The Top Resurgent CVEs Reveal About Attacker Priorities	20
Utility	20
Periodic	20
Black Swan	20

---

Recent Examples of Resurgence In The Wild	21
Surge in Palo Alto Networks Scanner Activity	21
Heightened Activity Targeting Key Edge Technologies	22
In-The-Wild Activity Against DrayTek Routers Amid Worldwide Reboots	22

---

How to Act on This Data: Strategic Next Steps for Security Professionals and Policymakers	23
For Security Professionals	23
For Policymakers	24

---

Appendix A: Methodology	25
-------------------------	----



# Key Takeaways

**1 Cyber threat actors from every corner of the world are exploiting resurgent vulnerabilities — often high-severity flaws affecting edge technologies.**

GreyNoise has identified and categorized three distinct classes of resurgent cyber vulnerabilities — each with their own unique set of behavioral characteristics and tendencies.

**2 Cyber vulnerabilities fall into four behavioral categories: Eternal (non-resurgent), and Utility, Periodic, and Black Swan (all resurgent).**

Each category exhibits unique behavior, presenting unorthodox threats to critical systems if not understood. Resurgent vulnerabilities have soared since 2017.

**3 Over half of the top exploited resurgent vulnerabilities affect edge technologies.**

Over 50% of the most exploited resurgent flaws, across all resurgent classes, affect edge technologies — the very systems attackers are relentlessly targeting in hopes of successfully breaching critical systems and data.

**4 Nearly 70% of the most unpredictable resurgent vulnerabilities (Black Swans) affect edge technologies.**

In our analysis, 67% of Black Swan CVEs affect edge systems — representing the largest proportion of all vulnerability categories.

**5 Some vulnerabilities are first exploited years after disclosure.**

Attackers first begin exploiting old vulnerabilities sometimes years after their publication date, presenting a significant blindspot for defenders.

**6 Nearly 40% of Black Swan vulnerabilities — those sparsely and infrequently targeted — affect routers and VPNs.**

Edge access points like routers and VPNs make up a large share of the most unpredictable resurgent CVEs.

**7 Resurgent vulnerabilities demand a rethink of security programs around patch management and dynamic blocking.**

Resurgent CVEs are often high-severity yet potentially overlooked — creating blind spots for defenders tasked with protecting critical systems.

**8 Government and private threat intelligence providers have reported state-sponsored exploitation of old vulnerabilities.**

While GreyNoise does not track attribution, we have continued to observe opportunistic activity targeting vulnerabilities that industry sources have linked to state-sponsored actors — highlighting their enduring appeal across a variety of threat actors.

**Resurgence (ri-'sər-jən(t)s):** a rising again into life, activity, or prominence.



# The Strategic Risk of Resurgent Vulnerabilities: How Dormant Threats Complicate Cyber Defense

Resurgent vulnerabilities pose an unorthodox threat to cyber defense — complicating how defenders patch vulnerabilities and detect emerging threats. These vulnerabilities, which can resurface after extended periods of inactivity, pose more than just a technical challenge; they are a strategic weakness actively exploited by opportunistic attackers from every corner of the world. GreyNoise's research shows that resurgent vulnerabilities disproportionately impact edge technologies — **the very systems threat actors are increasingly using to gain deep and persistent access to networks and data**. This pattern demonstrates the urgent need for proactive mitigation strategies, as the exploitation of resurgent vulnerabilities directly threatens organizational security.

To better understand the nature of resurgent vulnerabilities, GreyNoise conducted a comprehensive analysis, categorizing known exploited vulnerabilities based on their resurgence patterns. Our analysis revealed that resurgent vulnerabilities pose unique risks due to their unpredictable resurgence trends. These vulnerabilities can sit unpatched and ignored until adversaries rediscover or adapt them — often with little warning. This unpredictability makes Black Swan vulnerabilities especially concerning, as they can abruptly resurface, catching defenders off guard and enabling strategic exploitation by attackers.

Aware of the weaknesses inherent in edge security — and the broad access gained once compromised — **opportunistic attackers have incessantly targeted edge systems belonging to a broad set of technologies**. Major breaches and even attacks on critical infrastructure have relied on edge exploitation, providing threat actors with the footholds they need to successfully breach and exfiltrate data, deploy ransomware, and more.

**This report seeks to raise awareness of the challenges to cyber defense posed by resurgent vulnerabilities.** Their unpredictable nature, disproportionate impact on edge technologies, and tendency to include high-severity and overlooked low-severity vulnerabilities make them especially difficult to address. To mitigate these risks, security professionals must adopt proactive, intelligence-driven approaches to vulnerability management and threat detection, while policymakers must develop and implement frameworks to address these evolving threats.

# Defining Resurgent Vulnerabilities: A Behavioral Taxonomy

GreyNoise analyzed a dataset of known exploited vulnerabilities in internet-exposed systems published between 2010 and 2020, revealing they can be reduced to four main categories. Each category exhibits a unique set of characteristics presenting distinct threats to digital infrastructure.

The four categories of vulnerabilities in our analysis are:

## Eternal (Non-Resurgent)

<b>BEHAVIOR</b>	Characterized by consistent, ongoing exploitation with little fluctuation over time. They are continuously targeted by many IPs, showing persistent activity throughout the observed period. Organizations tend to prioritize defenses around these vulnerabilities given constant attacker interest.
<b>UNIQUE RISK</b>	Near instantaneous targeting once the system becomes exposed to the internet, experiencing a barrage of IP addresses with little to no dormancy in activity over time.
<b>EXAMPLE CVE</b>	<b>CVE-2017-5638 (Apache Struts Remote Code Execution)</b> This vulnerability gained global attention when it was exploited in the Equifax breach, impacting millions of individuals. Eight years later, GreyNoise continues to <u>observe</u> opportunistic activity against this vulnerability.

## Utility (Resurgent)

<b>BEHAVIOR</b>	Frequently exploited but with occasional breaks in activity. They are targeted regularly, but not constantly, reflecting ongoing relevance with occasional lulls.
<b>UNIQUE RISK</b>	Defenders might deprioritize them during quiet periods, leaving gaps when activity surges again.
<b>EXAMPLE CVE</b>	<b>CVE-2020-5902 (F5 BIG-IP TMUI RCE)</b> Utility vulnerabilities like <u>CVE-2020-5902</u> experience frequent exploitation with few periods of inactivity. The flaw was targeted quickly after disclosure but now exhibits resurgent behavior, presenting a dual challenge for defenders tasked with effectively prioritizing remediation efforts.

### Periodic (Resurgent)

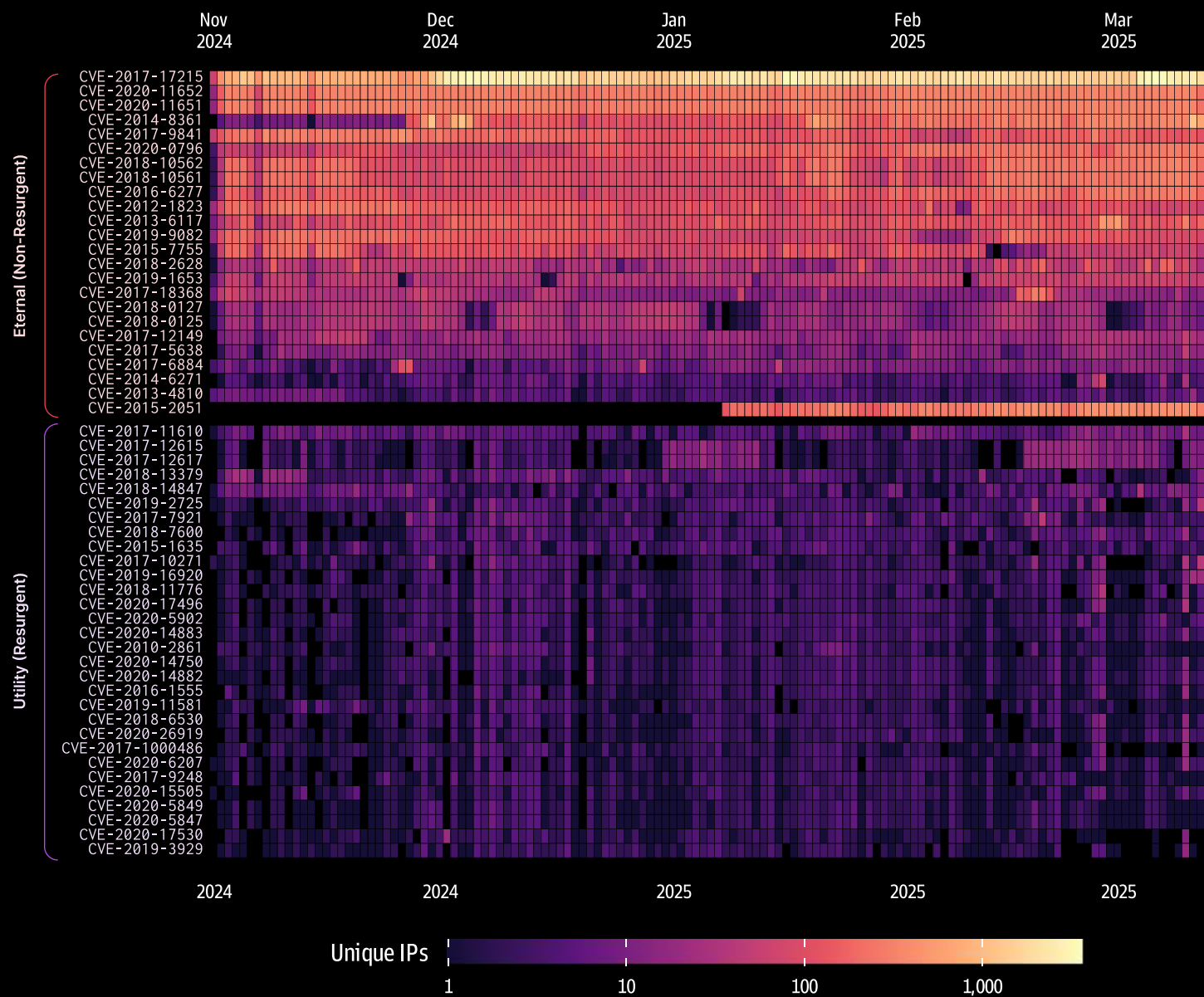
BEHAVIOR	Recurring patterns of exploitation. They are targeted in bursts, with clear but unpredictable intervals between each spike, indicating cyclical or campaign-driven exploitation.
UNIQUE RISK	Their irregular but recurring nature makes it challenging to predict the next wave, leading to potential complacency during inactive periods.
EXAMPLE CVE	<b>CVE-2019-3396 (Atlassian Confluence Template Injection)</b> Following an periodic pattern, GreyNoise continues to observe opportunistic activity against the flaw — ebbing and flowing in an unpredictable fashion that makes it difficult to prioritize.

### Black Swan (Resurgent)

BEHAVIOR	Mostly dormant, showing little to no activity for extended periods. However, they occasionally resurface with brief, sporadic exploitation, making their occurrence inordinately unpredictable.
UNIQUE RISK	Their sudden and unexpected resurgence can catch defenders off guard, as these vulnerabilities often appear irrelevant until they become active again.
EXAMPLE CVE	<b>CVE-2018-0171 (Cisco IOS XE Remote Code Execution)</b> This edge flaw exemplifies the Black Swan pattern. GreyNoise observes sporadic attacker interest in CVE-2018-0171 — typically dormant, then suddenly reappearing.

*Continued on next page...*

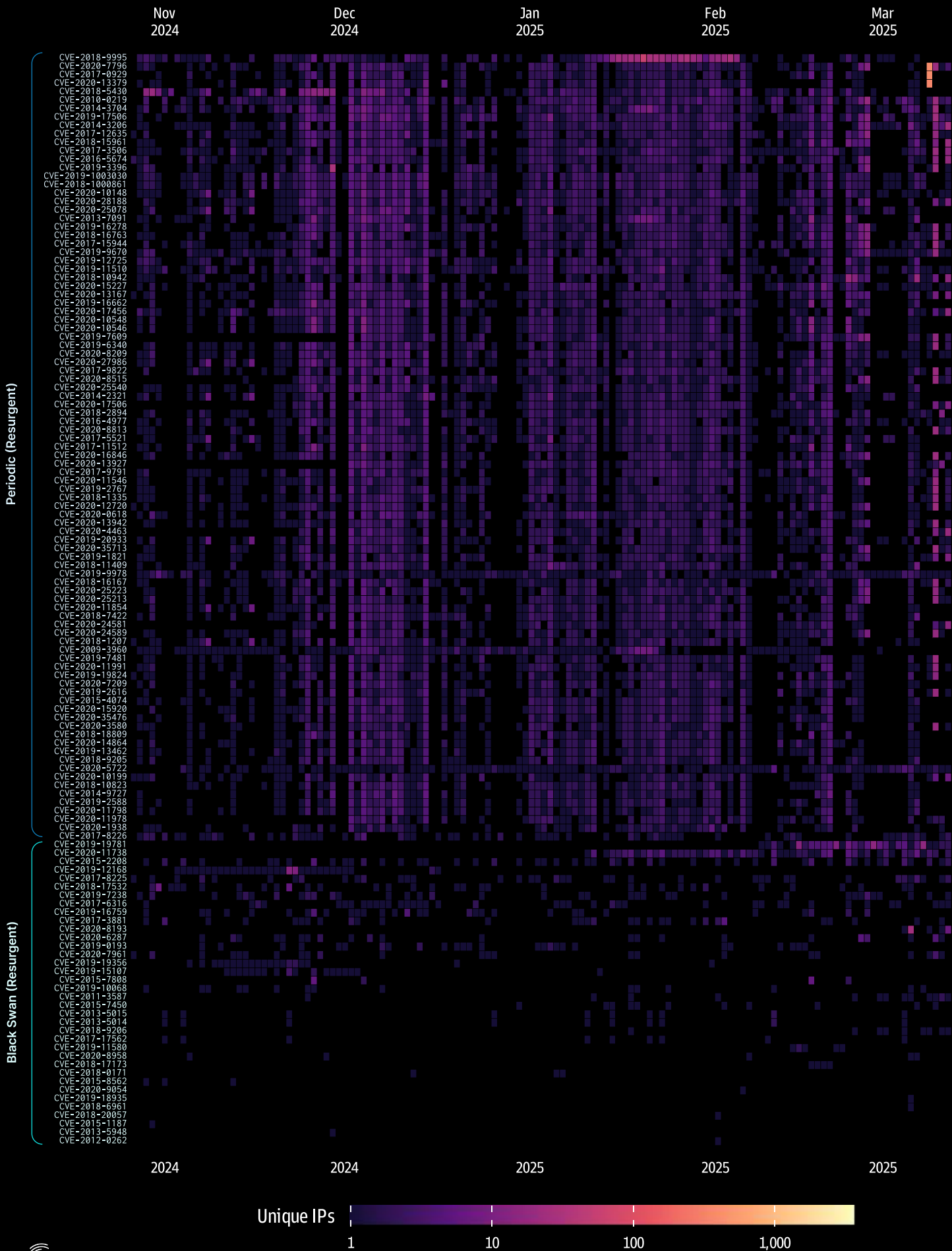
# GreyNoise Daily Observations For CVEs Published Between 2010 & 2020



Continued on next page...



# GreyNoise Daily Observations For CVEs Published Between 2010 & 2020



### Resurgence from a Different Perspective

The above resurgent categories — Utility, Periodic, and Black Swan — will be our main definitions of resurgence throughout the report; however, it's useful to assess resurgence from a variety of perspectives.

**The delta between a vulnerability's publication date and the creation of a GreyNoise tag tracking activity associated with that vulnerability is another way to assess resurgence.** The chart below shows that some vulnerabilities exhibit significant differences between publication date and GreyNoise tag creation — a measure of when a vulnerability reaches levels of activity warranting interest — while some experience near-instantaneous targeting after publication. In a sense, the greater the delta, the more resurgent the vulnerability — GreyNoise may not observe targeting of a CVE until years after its publication date. This creates risk for vital systems that go unpatched for years due to little attacker interest, only to face intense exploitation much later. The dark bars represent extreme cases of resurgence, indicating significant deltas between publication date and GreyNoise tag creation.

*Continued on next page...*

## Resurgence from a Different Perspective

The delta between a vulnerability's publication date and the creation of a GreyNoise tag tracking activity associated with that vulnerability is another way to assess resurgence. Shorter segments indicate a smaller delta between CVE creation and tag creation. Abrupt 'stops' at 2020 are the result of the birth of GreyNoise with a pre-established tag corpus.

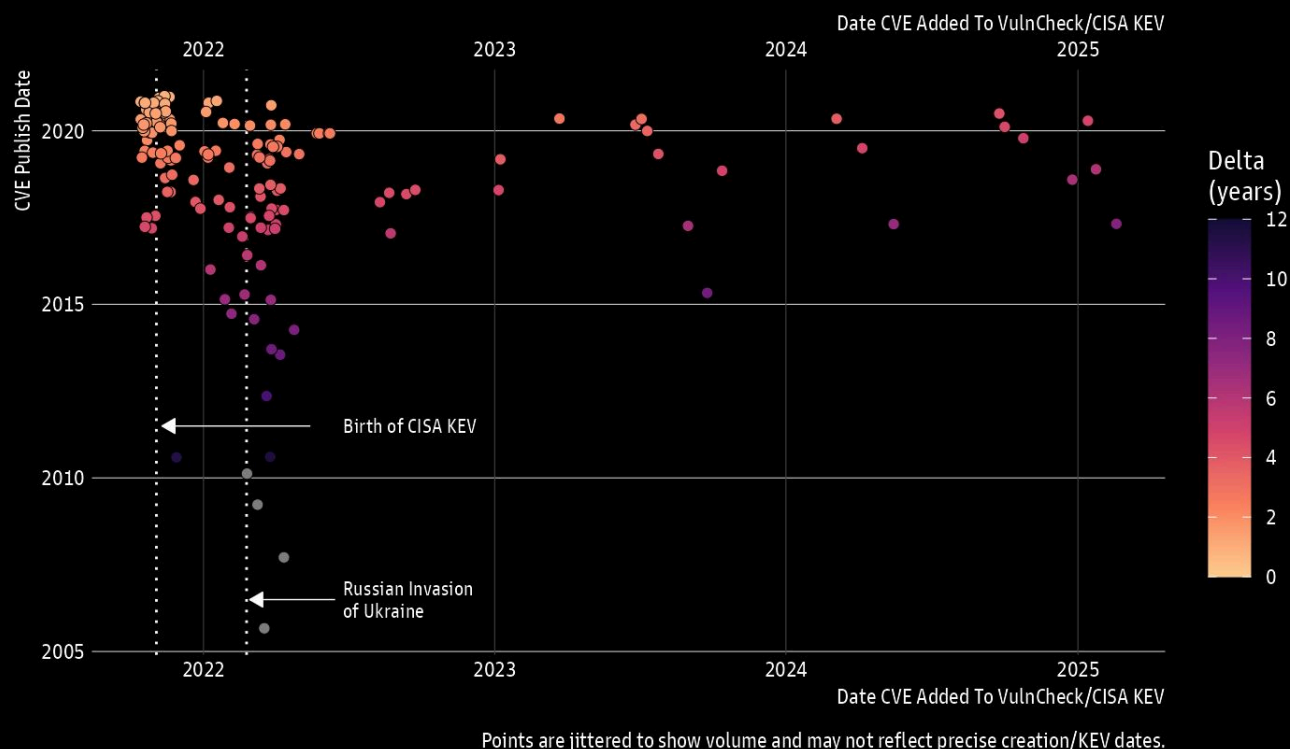


## Defining Resurgent Vulnerabilities: A Behavioral Taxonomy

The phenomenon of resurgence is also evidenced by the delta between a vulnerability's publication date and its addition to VulnCheck's Known Exploited Vulnerabilities (KEV) catalog, which includes all CISA KEVs. Since its introduction in 2021, CISA's KEV experienced a significant number of additions — notice the large number of additions in 2021 below. Another wave of additions appeared in 2022 after the Russian Federation's invasion of Ukraine.

### When Did CVEs Resurge Onto VulnCheck/CISA KEV?

The first few months of CISA's KEV program contained a massive initial dump of CVEs, with a second dump to aid in defending from cyberattacks from known weaponized CVEs used in the Russian invasion of Ukraine.



Continued on next page...



### Some Vulnerabilities Are First Exploited Years After Disclosure

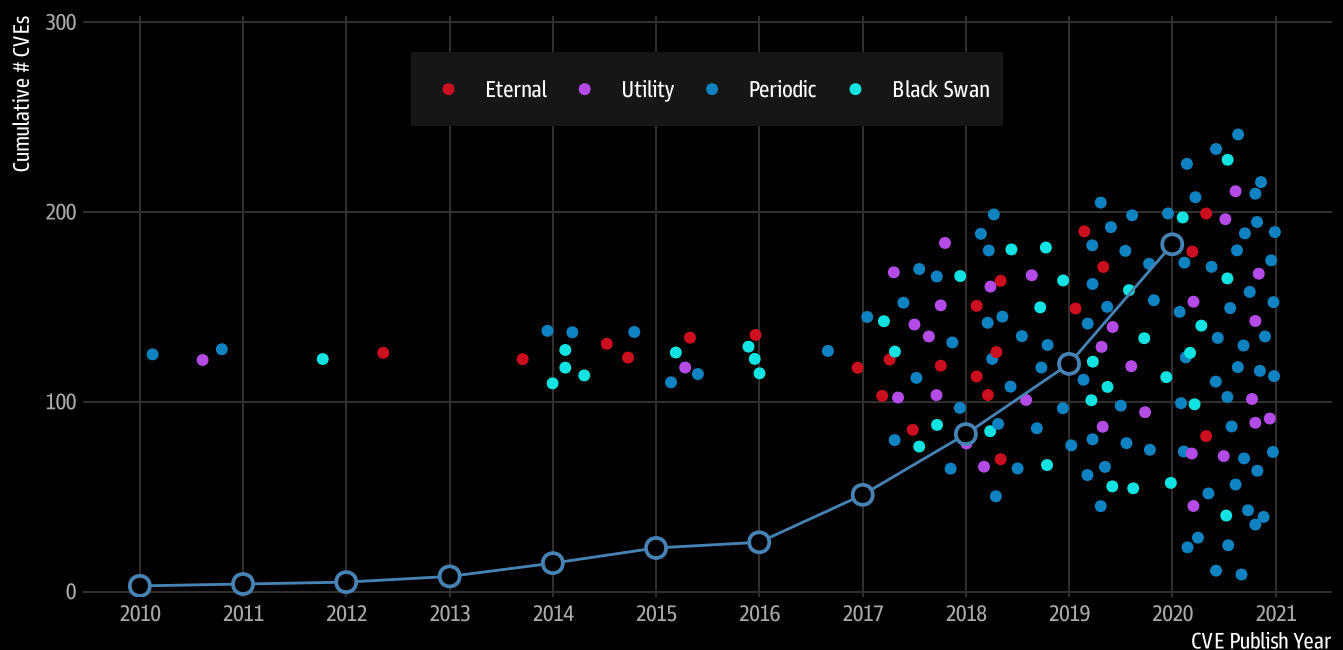
After these early additions, vulnerabilities were regularly added as “known exploited” years after their publication date. Some vulnerabilities from 2020 and before were first recognized as known exploited in or after 2024.

Both of these views of resurgence highlight a common challenge — **attackers first begin exploiting old vulnerabilities sometimes years after their publication date, presenting a significant blind spot for defenders.** This can cause organizations to forget about these vulnerabilities, and in some instances entirely deprioritize them based on lack of sustained targeting and resulting quiet in the media.

The macro view is also clear — resurgent vulnerabilities are rapidly rising, beginning their surge in 2017. The cumulative number of resurgent vulnerabilities over time is as follows:

### Published Resurgent CVE Volume Began To Soar In 2017

The macro view is clear — resurgent vulnerabilities are rapidly rising, beginning their surge in 2017



# A Critical Link: The Edge Connection

Resurgent vulnerabilities alone represent a serious risk to organizational security, but the gravity of this report's findings lie in resurgent vulnerabilities' close relationship with edge technologies — entry points into networks that, when compromised, can lead to significant disruption, exposure of sensitive information, and adversarial persistence in vital systems.

Our analysis revealed that some resurgent classes disproportionately affect edge technologies. The most striking overrepresentation was in the least predictable and most unique category — with **67% of Black Swan vulnerabilities affecting edge technologies**. In comparison, 52% of Eternal, 41% of Periodic, and 30% of Utility vulnerabilities affect edge technologies. The disparity between categories indicates that the edge-heaviness in Black Swans is not due to GreyNoise's data skewing toward edge systems. Instead, this finding suggests that **Black Swan vulnerabilities are uniquely edge-heavy, combining an unorthodox behavior (resurgence) with a technology type increasingly targeted by both opportunistic and advanced state actors.**

## A Critical Link: The Edge Connection

Edge technologies represent critical network entry points where Black Swan vulnerabilities pose an extraordinary threat.

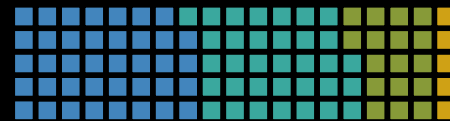
### Eternal



### Utility



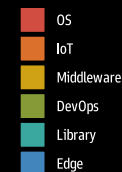
### Periodic



### Black Swan



#### Technology Type



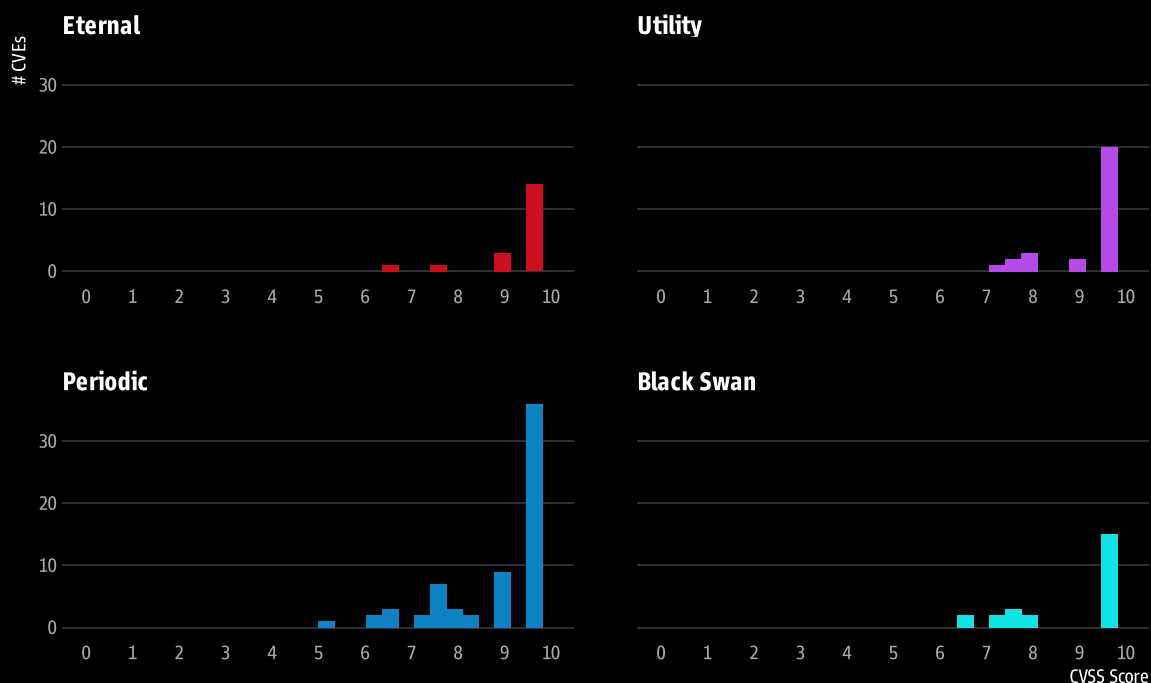
Continued on next page...

# Resurgent Vulnerabilities Skew Toward High-Severity

The distribution of Common Vulnerability Scoring System (CVSS) scores reveals another valuable piece of information — like Eternally-exploited vulnerabilities, all resurgent categories (Utility, Periodic, Black Swan) skew towards having high CVSS scores. In one sense, the high-severity skew validates that, regardless of targeting frequency or IP volume, known exploited vulnerabilities all tend to be clustered around higher CVSS scores.

## Resurgent Vulnerabilities Skew Toward High-Severity

Lower CVSS vulnerabilities make up a nontrivial portion of resurgent vulnerabilities — a double-edged sword of competing signals.



However, notice that lower CVSS vulnerabilities make up a nontrivial portion of resurgent vulnerabilities — a double-edged sword of competing signals:

- More severe resurgent vulnerabilities are more likely to be prioritized yet they may also be deprioritized based on long periods of dormancy, especially in the case of Black Swan vulnerabilities.
- Less severe resurgent vulnerabilities are less likely to be prioritized yet resurgent activity may catch defenders off guard.

This high-severity skew — especially among Black Swan vulnerabilities — is even more concerning given their disproportionate impact on edge technologies. This makes them attractive targets for opportunistic attackers seeking low-cost, straightforward ways to gain access to high-value systems and data.

Some of the flaws classified as resurgent in our analysis have been reportedly used in ransomware campaigns and attacks on critical infrastructure.

# Black Swan Vulnerabilities: The Most Router-Heavy Resurgent Category

Routers represent a unique risk to organizational security. With widespread adoption of work-from-home (WFH), organizations have expanded their attack surfaces to include their employees' home routers, and attackers are well aware of this vulnerability. GreyNoise consistently observes opportunistic attacks targeting home, industrial, and enterprise routers. Additionally, **these devices often serve as low-profile infrastructure for attackers to obfuscate and launch their attacks, as they are often beyond the purview of enterprise security teams.**

We found that Black Swan vulnerabilities disproportionately affect routers and VPNs, more than any other resurgent category. Over **36% of Black Swan vulnerabilities affect routers**, compared to 27% for Utility and 22% for Periodic. Notably, almost 50% of Eternal vulnerabilities — which are not resurgent by definition — affect routers or VPNs, representing the largest share among vulnerability categories.

This finding raises a dual set of concerns. **Not only do defenders need to treat routers as critical entry points for attackers, but they must also contend with the unpredictable nature of resurgent vulnerabilities found in routers, particularly Black Swans.** Attacker activity targeting these flaws can remain dormant for long periods before resurfacing, complicating patch prioritization and defense strategies. Black Swan vulnerabilities' sporadic and unexpected exploitation patterns make consistent protection challenging, leaving routers vulnerable to sudden attacks.

While Eternal vulnerabilities are well-known and consistently targeted, Black Swan vulnerabilities may be more likely to slip through the cracks. The fact that many of these vulnerabilities affect routers means defenders should ensure they receive ample attention.

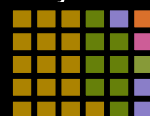
## Black Swan Vulns: The Most Router-Heavy Resurgent Category

Over 36% of Black Swan vulnerabilities affect routers, compared to 27% for Utility and 22% for Periodic. Notably, almost 50% of Eternal vulnerabilities — which are not resurgent by definition — affect routers or VPNs, representing the largest share among vulnerability categories.

### Eternal



### Utility



### Periodic



### Black Swan



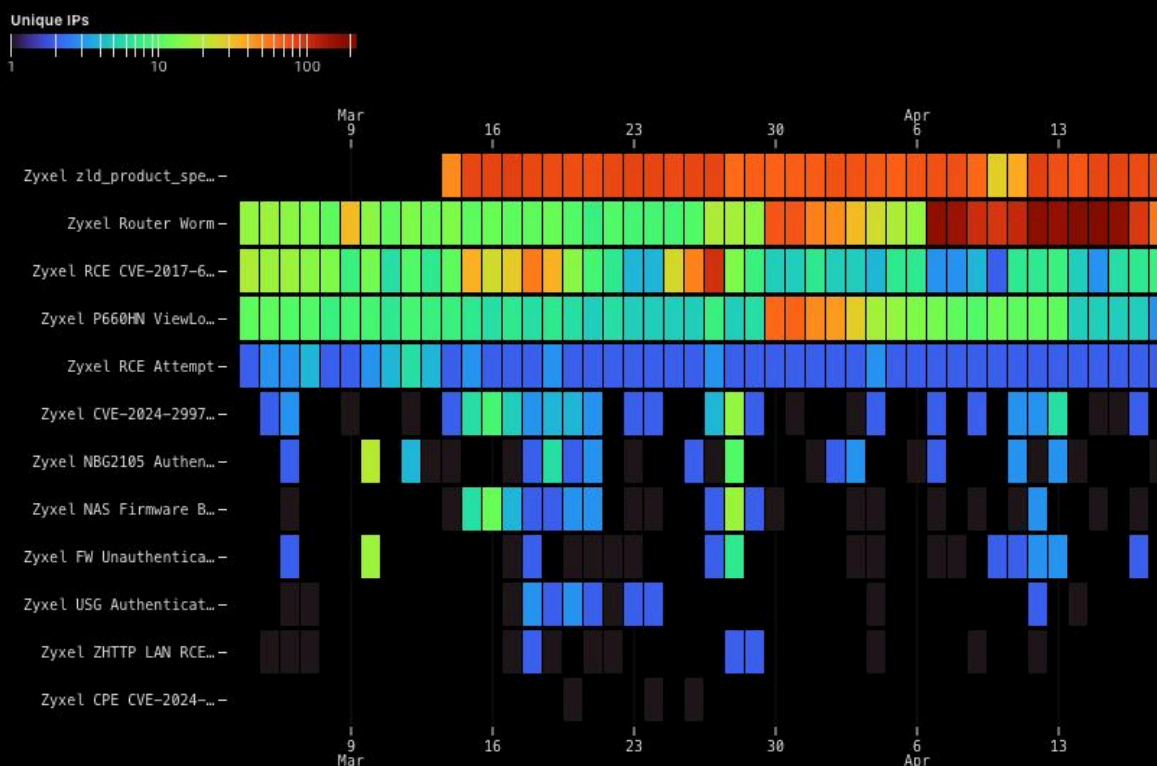
- File Share
- Firmware
- DVR
- Camera
- NAS
- Database
- OS
- CMS
- Router/VPN
- Application

### A Security Blindspot: Attackers Exploit Small Business Gear

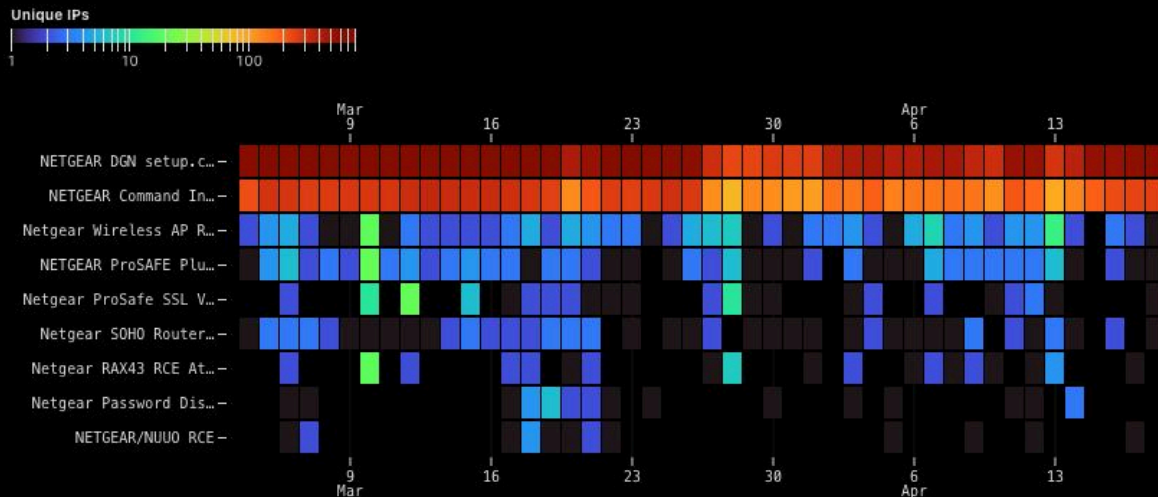
Aware of typically lower security standards, attackers are targeting old and outdated equipment commonly used by small and medium-sized businesses (SMBs), including routers. Small businesses rely every day on gear from NETGEAR, Cisco, Zyxel, and other vendors — representing a sizable portion of the available equipment attackers can use for obfuscation, botnet enlistment, ransomware, and other activities. **GreyNoise can confirm active exploitation across these technologies in the past 45 days:**

Leaders should recognize this vulnerability as a critical one, especially given the significant digital footprint SMBs represent. Some have theorized that a buy-back program — where the government purchases old and vulnerable equipment from SMBs — could incentivize the use of more secure technologies. Such a program could reduce the vulnerable digital footprint SMBs represent, thereby shrinking the attack surface available to opportunistic threat actors.

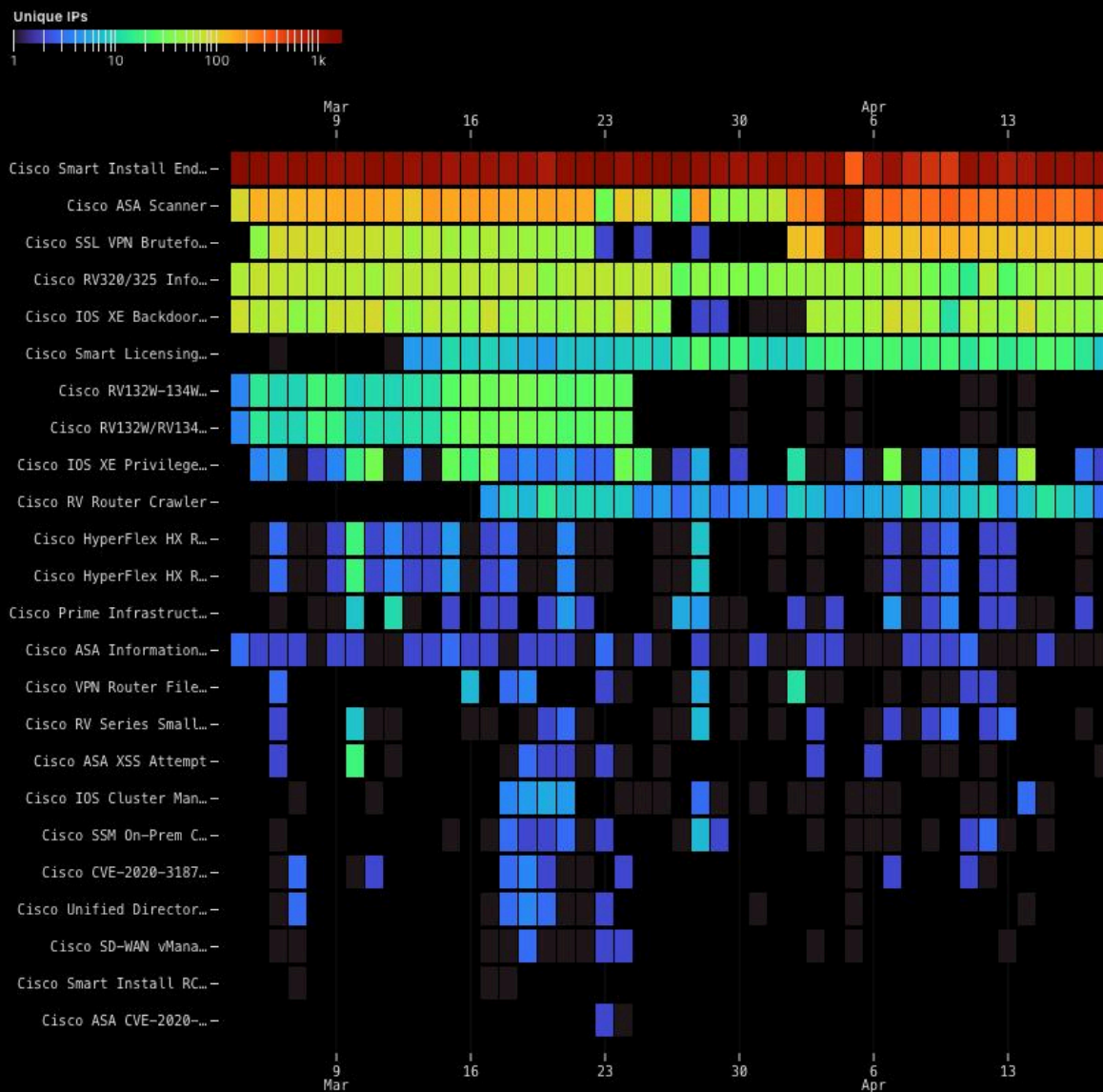
Zyxel Activity Heatmap



## Netgear Activity Heatmap



## Cisco Activity Heatmap











# Resurgence Demands a Rethink of Patch Management

The reappearance of old vulnerabilities in active exploitation reshapes how we think about patching. For years, vulnerability management programs have relied on a forward-looking model — prioritizing new disclosures, recent advisories, and severity scores. But resurgent vulnerabilities, and their accompanying qualities, flip that model.

This creates several challenges for vulnerability management teams:

-  **False Sense of Closure:** Once a vulnerability drops off the radar, it's often deprioritized — even if it remains unpatched in the environment.
-  **Swift & Delayed Exploitation:** Some vulnerabilities are first exploited years after disclosure — well after the initial push to patch them has faded — while others are near-instantly targeted post disclosure. The distribution of these deltas is continuous, leaving defenders to grapple with a variety of behaviors, not just two extremes.
-  **Defense Beyond Patching:** Sometimes taking a system offline isn't an option — operational costs, business continuity, and other factors make it infeasible. Dynamic IP blocking — a pre-patching emergency countermeasure or for when patching isn't realistic — can help protect critical systems from known-malicious IPs that are actively exploiting a given vulnerability.
-  **Edge Exposure:** Many resurgent CVEs affect edge technologies like routers, VPNs, and firewalls — systems that can provide attackers with access to critical systems and data if successfully exploited.
-  **Signal Sensitivity & Integrity:** Without primary, real-time visibility into renewed attacker interest, teams may miss the moment when a dormant threat becomes urgent again or chase false positives based on secondary, inaccurate intelligence.
-  **Inventory and Coverage Gaps:** Legacy systems and third-party infrastructure may still harbor years-old vulnerabilities that are no longer actively tracked — leaving teams blindsided when attackers suddenly begin exploiting them again

For these reasons, **resurgence is a core operational risk with which vulnerability management and threat detection teams must contend.** The challenge is not only identifying which old vulnerabilities might come back, but also recognizing when they do, and optimizing detection and remediation efforts accordingly. This process becomes more complex and sensitive when some resurgent vulnerabilities — Black Swans — subtly and unpredictably reappear, leaving a faint signal to shift priorities that could be missed without proper visibility.

# What The Top Resurgent CVEs Reveal About Attacker Priorities

The most exploited vulnerabilities in each resurgent category offer a window into how attackers prioritize access. While each category reflects a different pattern of exploitation — from constant pressure to sudden reappearances — these CVEs show which technologies and flaws remain favored targets across campaigns.

**More than 50% of the most exploited resurgent vulnerabilities across each category affect edge technologies.**

## Utility

*Utility CVEs reflect attackers' reliance on dependable access points across common technologies — including VPNs, middleware, and small office routers widely used by SMBs. These vulnerabilities remain persistent fixtures in exploitation activity, appearing repeatedly across campaigns.*

**CVE-2017-12617** (Apache Tomcat RCE)  
**CVE-2018-13379** (Fortinet FortiOS SSL VPN Path Traversal)  
**CVE-2018-14847** (MikroTik Router OS Directory Traversal)  
**CVE-2017-12615** (Apache Tomcat RCE)  
**CVE-2017-11610** (supervisord supervisor Incorrect Default Permissions)  
**CVE-2017-12615** (Apache Tomcat RCE)

## Periodic

*The top five span DVRs, Windows Infrastructure, monitoring tools, and email platforms — systems deployed across SMBs, enterprises, and public sector environments. Their cyclical exploitation makes them easy to overlook during quiet periods — until attackers return.*

**CVE-2018-9995** (tbkvision tbk-dvr4216\_firmware Improper Authentication)  
**CVE-2020-7796** (Synacor Zimbra Collaboration SSRF)  
**CVE-2017-0929** (dnnsoftware dotnetnuke SSRF)  
**CVE-2020-13379** (Grafana Labs Grafana SSRF)  
**CVE-2018-5430** (TIBCO JasperReports Server Information Disclosure)

## Black Swan

*The top Black Swan CVEs show how vulnerabilities with little prior attacker interest can suddenly become high-impact threats. From Citrix infrastructure to IP cameras and WordPress plugins, Black Swan vulnerabilities show how even obscure flaws can be widely targeted in unpredictable surges of activity.*

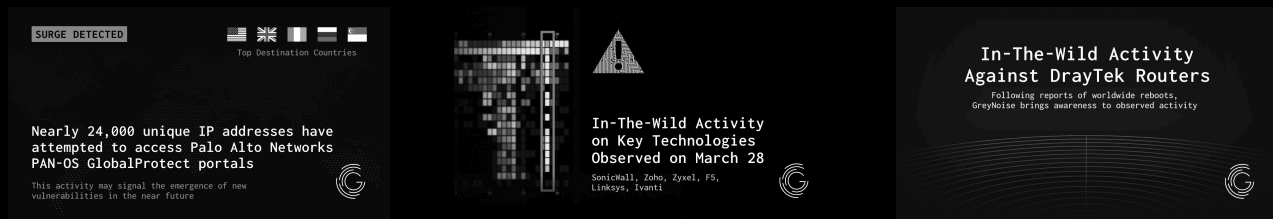
**CVE-2019-19781** (Citrix ADC, Gateway, and SD-WAN WANOP Appliance Code Execution)  
**CVE-2020-11738** (WordPress Snap Creek Duplicator Plugin File Download)  
**CVE-2015-2208** (avinu phpMyAdmin)  
**CVE-2019-12168** (four-faith f3x24\_firmware Missing Authorization)  
**CVE-2017-8225** (wificam wireless\_ip\_camera\_(p2p)\_firmware)

**Given that more than half of the top exploited resurgent vulnerabilities affect edge technologies, defensive strategies must match the scale and persistence of exploitation targeting these systems.**





# Recent Examples of Resurgence In The Wild



GreyNoise has been reporting on resurgent activity observed across its Global Observation Grid, a planetary-scale network of worldwide sensors. We've aggregated this reporting and other insights at the [GreyNoise blog](#). Here are a few salient examples:

## Surge in Palo Alto Networks Scanner Activity

On March 31, 2025, GreyNoise [reported](#) it had observed a significant surge in login scanning activity targeting Palo Alto Networks PAN-OS GlobalProtect portals. After days of near-zero attacker activity, our telemetry alerted us to nearly 24,000 IP addresses targeting Palo Alto Networks PAN-OS GlobalProtect login portals. The overwhelming majority of traffic targeted systems based in the United States, allowing defenders to prepare for what could be an early indication of upcoming threats.

Resurgence in scanning can serve as a potential indicator of future exploitation. GreyNoise's Bob Rudis — VP of Data Science & Security Research — added context in the report, saying:

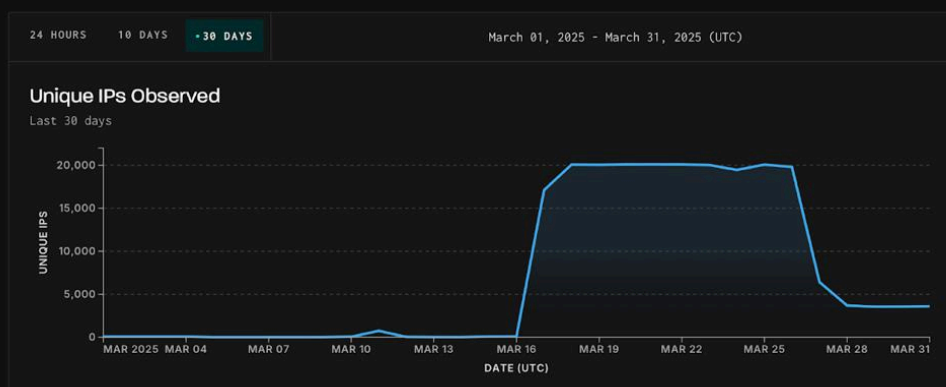
*“Over the past 18 to 24 months, we’ve observed a consistent pattern of deliberate targeting of older vulnerabilities or well-worn attack and reconnaissance attempts against specific technologies. These patterns often coincide with new vulnerabilities emerging 2 to 4 weeks later.”*

Resurgence in the wild takes many forms. In this case, a specific type of activity targeting Palo Alto Networks equipment appeared seemingly out of nowhere. The reporting quickly hit the headlines, and defenders scrambled to defend their networks given the news.

### 🚩 Palo Alto Networks Login Scanner

CATEGORY INTENTION  
🚩 Activity SUSPICIOUS

IP addresses with this tag have been observed attempting to login to Palo Alto Networks PAN-OS global-protect login portal.



23,958

Observed IPs →

- > Export IPs
- > Manage alert
- > View integrations
- > Block at firewall

#### CVEs:

No associated CVEs

#### Related Tags:

No related tags

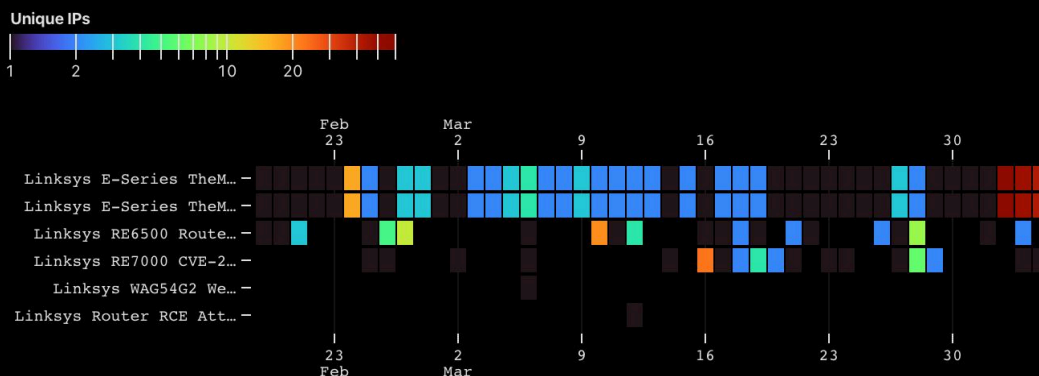


### Heightened Activity Targeting Key Edge Technologies

On March 28, 2025, GreyNoise observed a significant spike in activity targeting several key technologies, including SonicWall, Zoho, Zyxel, F5, Linksys, and Ivanti systems. Various vulnerabilities affecting these systems were targeted on the same day, apparently in unison.

One of the technologies hit by the surge was Linksys E-Series routers. After our initial reporting, we observed four days of inactivity followed by a sharp rise in targeting sustained for three days.

Linksys Activity Heatmap

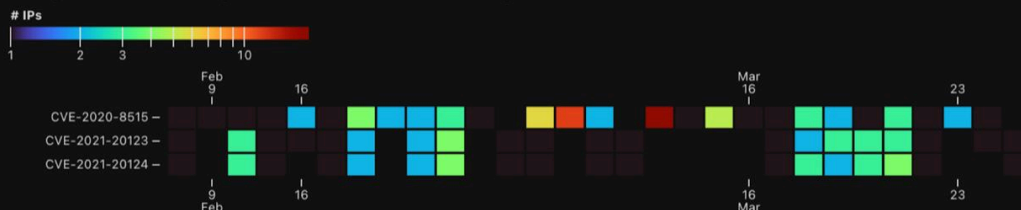


### In-The-Wild Activity Against DrayTek Routers Amid Worldwide Reboots

On March 25, 2025, GreyNoise was made aware of reports alerting the security community to mysterious DrayTek router reboots occurring worldwide. Actively tracking several vulnerabilities affecting these routers, we publicly shared intelligence indicating that some were being actively targeted by attackers, a potential explanation for the reboots — all three flaws in our report were from 2021 or earlier.

If it wasn't for reports of worldwide reboots, the community may have never been alerted to resurgent activity targeting DrayTek routers. Related or not to the reboots, headlines quickly spread the news, enabling defenders to take defensive actions.

GreyNoise 45-Day Observed CVE Activity



In-the-wild resurgence poses a threat to the security of our digital infrastructure. Emerging seemingly out of nowhere, attackers exploit old, overlooked, and newly discovered vulnerabilities alike — precisely targeting critical systems and edge technologies.

# How to Act on This Data: Strategic Next Steps for Security Professionals and Policymakers

GreyNoise's analysis of resurgence is an essential resource for security professionals and policymakers, offering the insights needed to anticipate and mitigate these unpredictable threats. By understanding how and why resurgent vulnerabilities are exploited, we can build a more resilient cyber defense strategy — one that proactively addresses not just the known risks but also the unexpected.

Now is the time to confront the evolving threat landscape with decisive and informed action. The following recommendations outline essential steps to strengthen our defense against the resurgence phenomenon, securing organizational security with improved defensive measures and policy actions.



## For Security Professionals

- 1 Enhance Real-Time Visibility into Edge Exploitation**  
With edge technologies prime targets for opportunistic attackers, maintaining visibility into real-time exploitation patterns is essential. Incorporate threat intelligence solutions that provide near-instant notice of resurgent activity, with accompanying metadata needed for proactive defense.
- 2 Dynamically Block Threat IPs**  
Resurgence means attacker interest ebbs and flows, leaving static blocklists useless when new threat IPs begin exploiting a given flaw. Defenders must leverage dynamic blocklists grounded in primary-sourced data to effectively and accurately block threats without disrupting business operations.
- 3 Strengthen Incident Response for Resurgent Threats**  
Build incident response protocols specifically for vulnerabilities in edge systems, accounting for the unpredictable nature of resurgent exploitation. Leverage real-time data from tools enabling faster detection and response when previously dormant vulnerabilities resurface.
- 4 Leverage Real-Time Intelligence to Inform Patching Decisions**  
Rather than relying solely on severity scores, integrate intelligence that highlights current exploitation activity into your patching cadences. This approach ensures that patch prioritization is based on real-world data, helping defenders stay ahead of resurgent threats — particularly those affecting edge technologies.

Private and public sector defenders share the responsibility of protecting critical systems from all threats, including those highlighted in this report. With approximately 85% of U.S. critical infrastructure owned by the private sector, collaboration between public and private stakeholders is crucial to safeguarding organizational security. This places a significant burden on private sector defenders — including CISOs, SOC analysts, incident responders, threat hunters, and others — to take decisive action against unorthodox risks to organizational security.





### For Policymakers

- 1 Prioritize Edge Exploitation as a Security Imperative**  
Edge technologies are being heavily targeted, often using high-severity vulnerabilities allowing for deep access to networks and data if successfully exploited. Resurgent attacker interest in these flaws — coupled with the broad access they provide attackers — makes them a critical threat to organizational security, data privacy, and more.
- 2 Advocate for Real-Time Monitoring for Critical Infrastructure**  
Advocate for critical infrastructure operators to implement real-time threat intelligence solutions, especially those capable of identifying resurgent exploitation and providing information necessary for immediate defense.
- 3 Facilitate Collaboration with Cybersecurity Experts**  
Establish ongoing collaboration channels between threat intelligence experts, critical infrastructure operators, and national security agencies to continuously assess and respond to resurgent threats.
- 4 Survey Your Country's Attack Surface**  
Convene with experts to map your nation's attack surface, revealing potential blindspots and areas of disproportionate risk. Evaluate how much of your nation's digital infrastructure depends on edge and small business technologies to inform risk-reduction policies — and consider buy-back programs for outdated or vulnerable technologies.

Policymakers play a crucial role in safeguarding national and organizational security by addressing the risk posed by resurgent vulnerabilities, particularly those targeting edge technologies. As attackers increasingly exploit these flaws, it is essential for policymakers to take a proactive stance. To develop effective policies, policymakers must actively collaborate with cybersecurity experts, critical infrastructure stakeholders, and intelligence communities. Taking decisive and coordinated action — leveraging partnerships between the public and private sectors — is essential to strengthening our defenses against these threats. **The security of our critical infrastructure depends on proactive measures to mitigate resurgent vulnerabilities.**

# Appendix A: Methodology

---

GreyNoise reviewed threat actor activity observations against CVEs identified in [VulnCheck's Known Exploited Vulnerabilities catalog](#), as it is more comprehensive than [CISA's Known Exploited Vulnerabilities catalog](#). We further identified all CVEs we have [tag coverage](#) for and used data from our Global Observation Grid across the period of November 2024 to March 2025.

The CVE categories — “Eternal”, “Utility”, “Periodic”, and “Black Swan” — are based on observation frequency and consistency of contacts. “Utility,” “Periodic” and “Black Swan” categories were grouped together into the definition of “resurgent” due to their sporadic activity. The majority of “Periodic” resurgent vulnerabilities have similar attack frequency and magnitude characteristics, which suggest they are likely being focused on by one or more similar botnets or controlled by the same adversaries.

The categorizations in the faceted waffle charts are based on [this metadata](#) compiled by GreyNoise.



# 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](https://greynoise.io/contact/sales)