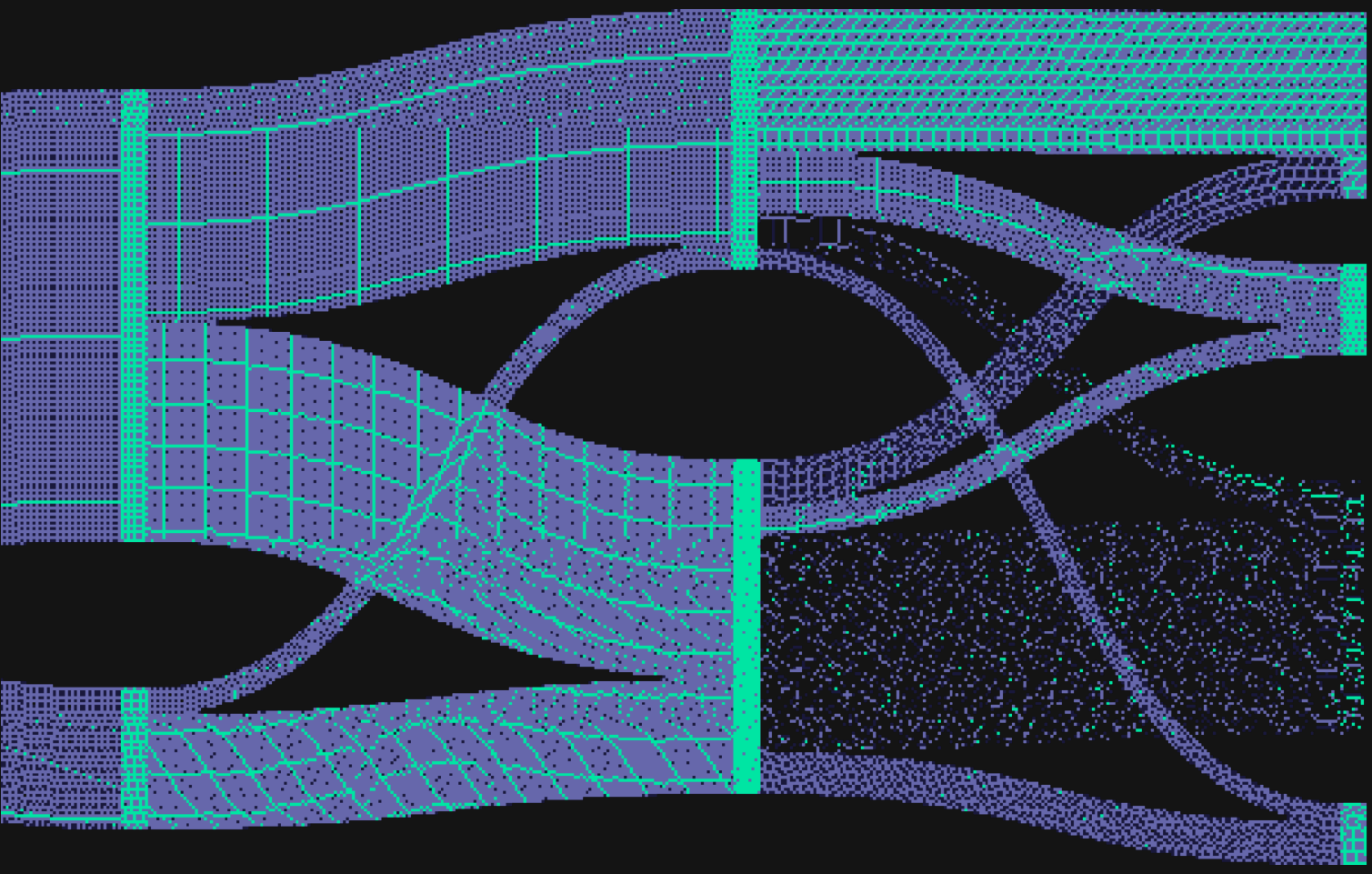
2026 State of Exploitation:

# Exploring the Network Edge

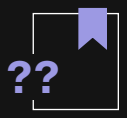
## The Risk of End-of-Life Infrastructure



VulnCheck

# Key Findings

**42.5% of vulnerabilities exploited in 2025 affected devices that are end of life or likely end of life**, with additional vulnerabilities affecting products that have already reached end of sale.



**Many exploited edge device vulnerabilities are not represented in CISA KEV:** Only 23.7% of the exploited edge device vulnerabilities identified by VulnCheck appear on CISA KEV.

**Consumer networking equipment is a major exploitation target:** Consumer routers and globally distributed networking products account for a 56% of exploited edge device vulnerabilities.

**Active exploitation frequently precedes CVE assignment:** VulnCheck issued CVEs for 18 vulnerabilities after detecting exploitation activity through honeypots and canary systems.

**Botnets disproportionately target unsupported devices:** 65% of vulnerabilities exploited by botnets affect end of life or likely end of life products.

## About the Report

Network edge devices play a critical role in modern infrastructure, yet many remain deployed long after vendors stop supporting them. On February 5, 2026, the Cybersecurity and Infrastructure Security Agency (CISA) published **Binding Operational Directive 26-02 (BOD 26-02)**, Mitigating Risk From End of Support Edge Devices.

This prompted us to examine whether vulnerabilities being actively exploited disproportionately affect end-of-life or unsupported edge devices. Analysis shows that attackers frequently target this aging infrastructure, particularly through botnets exploiting widely deployed consumer networking devices.

## Methodology

We examined vulnerabilities added to VulnCheck KEV in 2025 from our **2026 State of Exploitation Report** that we categorized as network edge devices. Network edge devices are hardware or software systems that are typically internet-facing and located at the boundary between an internal network and external networks such as the internet, cloud services, or partner networks. These devices manage, control, and secure the flow of data entering and leaving the network.

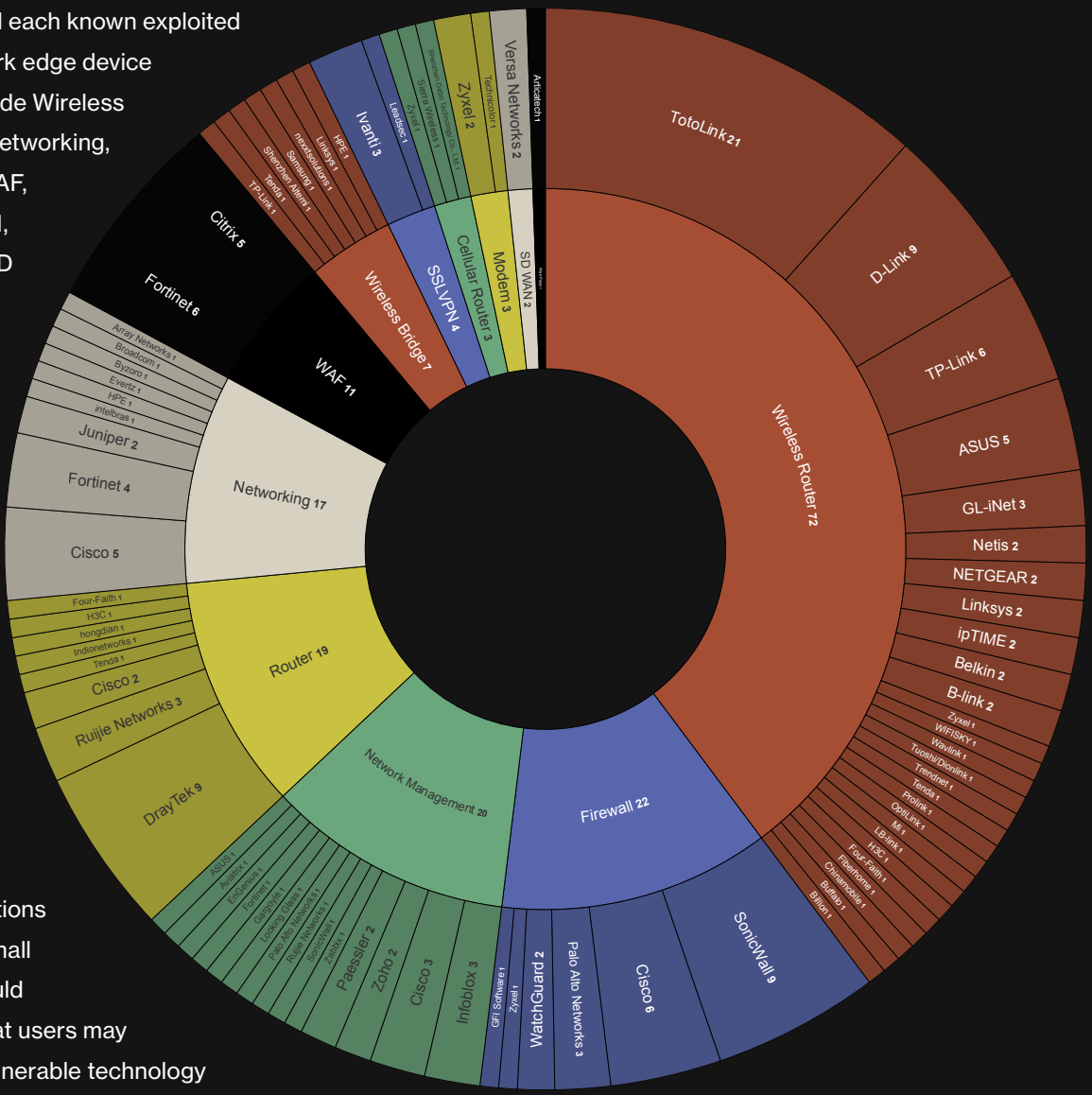
For this analysis, we used the 181 known exploited vulnerabilities that we identified as network edge devices in our 2026 State of Exploitation report. We enriched this dataset with end of life information, software producer details (including company headquarters), and additional threat intelligence beyond what is available in VulnCheck KEV.

# Edge Devices Are Attractive Targets

Network edge devices are often targeted by attackers because they are internet facing, widely deployed, and often poorly maintained. Consumer networking devices, in particular, may remain in service for many years without firmware updates, making them persistent targets for botnet operators and other attackers.

## Exploited Network Edge Devices by Device Type

We also explored exploited vulnerabilities by device type. To do this, we categorized each known exploited vulnerability by the network edge device type. The categories include Wireless Router, Router, Firewall, Networking, Network Management, WAF, Wireless Bridge, SSL VPN, Modem Cellular Router, SD WAN, and Web Proxy. This categorization highlights the broad range of network edge devices and vendors being targeted.




One clear pattern through our analysis is the volume of consumer routers being targeted, beyond the traditional enterprise devices more commonly discussed in enterprise security circles. Organizations with remote workers or small branch/home offices should consider the likelihood that users may connect through older, vulnerable technology that the organization has limited visibility into.

# Exploited Edge Devices by Support Status

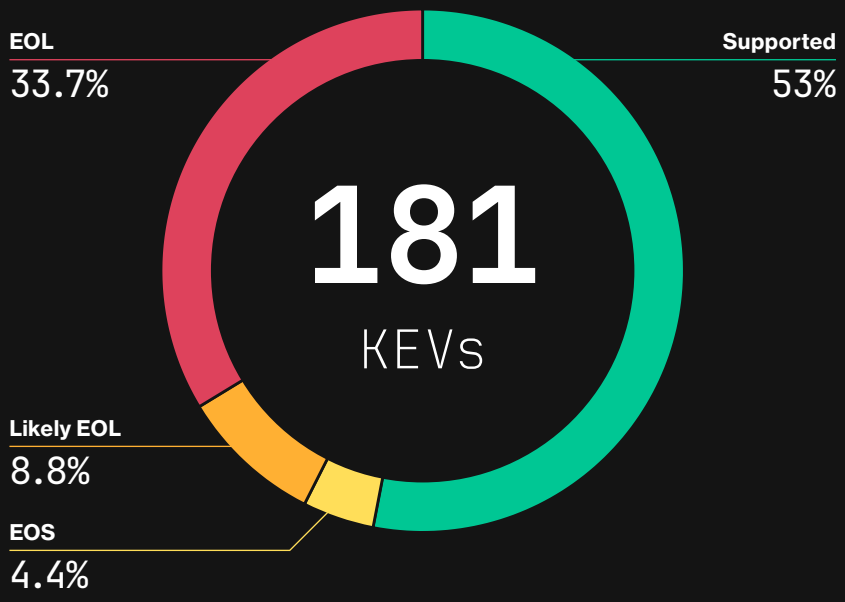
## (EOL Problem)

On February 5, 2026, the Cybersecurity and Infrastructure Security Agency (CISA) published **Binding Operational Directive 26-02 (BOD 26-02)**, Mitigating Risk From End of Support Edge Devices. This prompted us to examine whether vulnerabilities being actively exploited disproportionately affect end-of-life or unsupported edge devices.

Of the 181 network edge device vulnerabilities added to VulnCheck KEV in 2025, 42.5 percent were associated with end of life (EOL) or likely EOL devices. An additional 4.4 percent were associated with devices that are at the end of sale and approaching end of life.

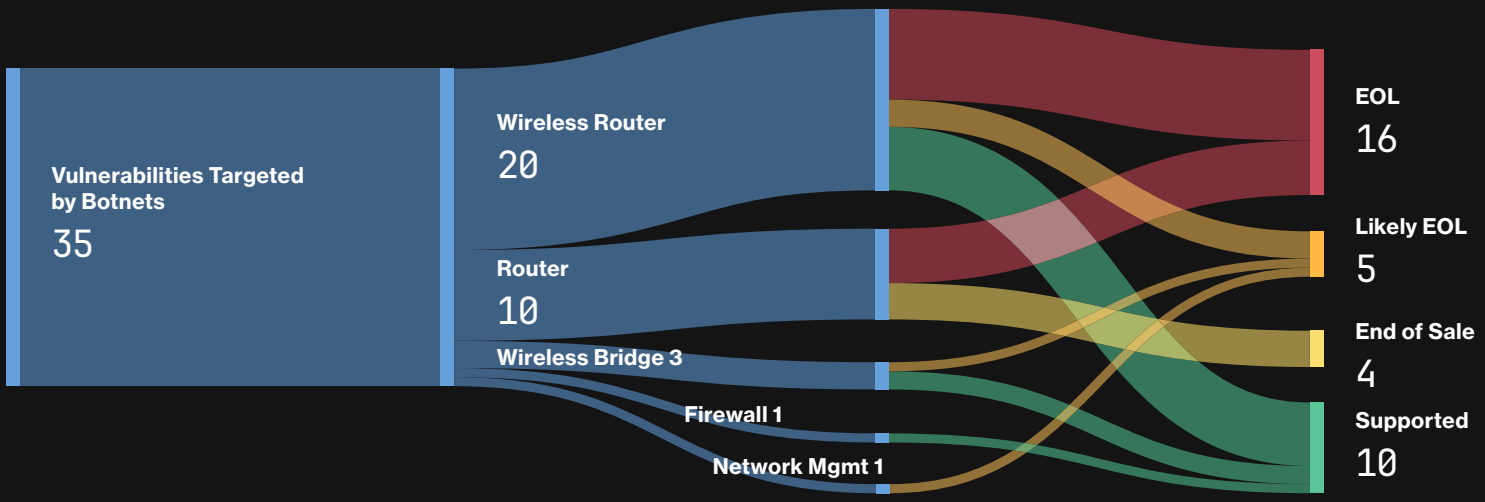
These findings suggest that unsupported infrastructure remains a persistent attack surface for both opportunistic botnets and targeted attackers.

EOL Status of Network Edge Devices: VulnCheck KEV



# Network Edge Devices Botnets Target

Thirty-five of the 181 network edge device KEVs added to VulnCheck KEV in 2025 (19 percent) were known to be targeted by botnets. Botnets disproportionately target unsupported infrastructure. Sixty-five percent of vulnerabilities exploited by botnets affect devices that are end of life or likely to be end of life. Only five of these CVEs targeted by botnets are included in CISA KEV.




## Edge Device Ransomware Attribution

Seven of the 181 KEVs were associated with ransomware campaigns, all of which are tied to enterprise network edge devices. None of these vulnerabilities have attribution to botnets, which is an interesting contrast. Botnets appear more likely to target widely deployed consumer devices.

| CVE | Vendor | Product |
|---|---|---|
| CVE-2025-24472 | Fortinet | FortiOS and FortiProxy |
| CVE-2025-23006 | SonicWall | SMA1000 Appliances |
| CVE-2025-22457 | Ivanti | Connect Secure, Policy Secure, and ZTA Gateways |
| CVE-2025-5777 | Citrix | NetScaler ADC and NetScaler Gateway |
| CVE-2024-53704 | SonicWall | SonicOS |
| CVE-2025-0282 | Ivanti | Connect Secure, Policy Secure, and ZTA Gateways |
| CVE-2024-55591 | Fortinet | FortiOS and FortiProxy |

# Network Edge Device Vulnerabilities in CISA KEV

Of the 181 network edge device KEVs identified by VulnCheck, 43 (23.7 percent) are included in CISA KEV.

A review of the data suggests a few reasons for the lower representation in CISA KEV, and more specifically, the lower prevalence of end of life network edge devices.

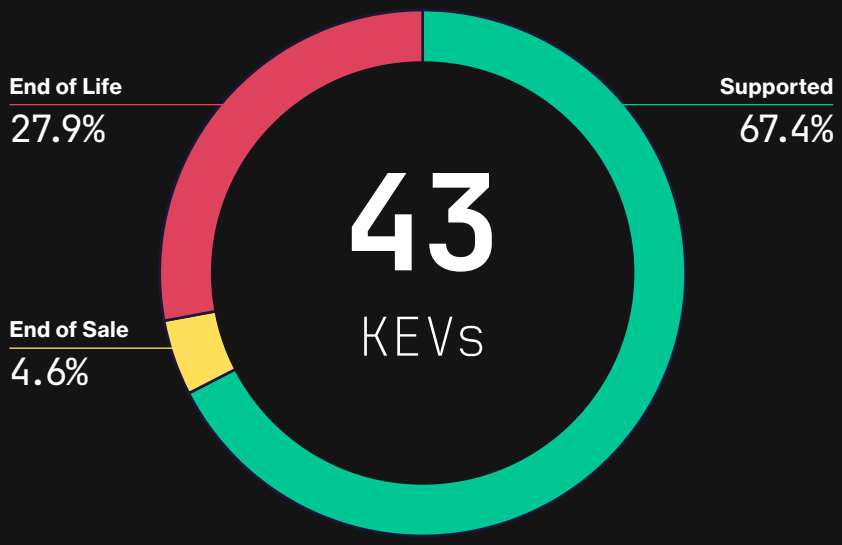
First, many products are manufactured and sold primarily for markets outside the United States and may fall outside CISA's primary scope. Totolink, for example, is a Chinese company that sells products primarily across Asian markets.

Second, end of life devices may be less likely to be added to CISA KEV because there is often no available fix, which is a requirement for inclusion. In cases where CISA KEV has included end of life devices, the guidance generally states that organizations should discontinue use of the product if mitigations are unavailable.

Third, consumer-grade edge devices are less likely to be present on federal networks.

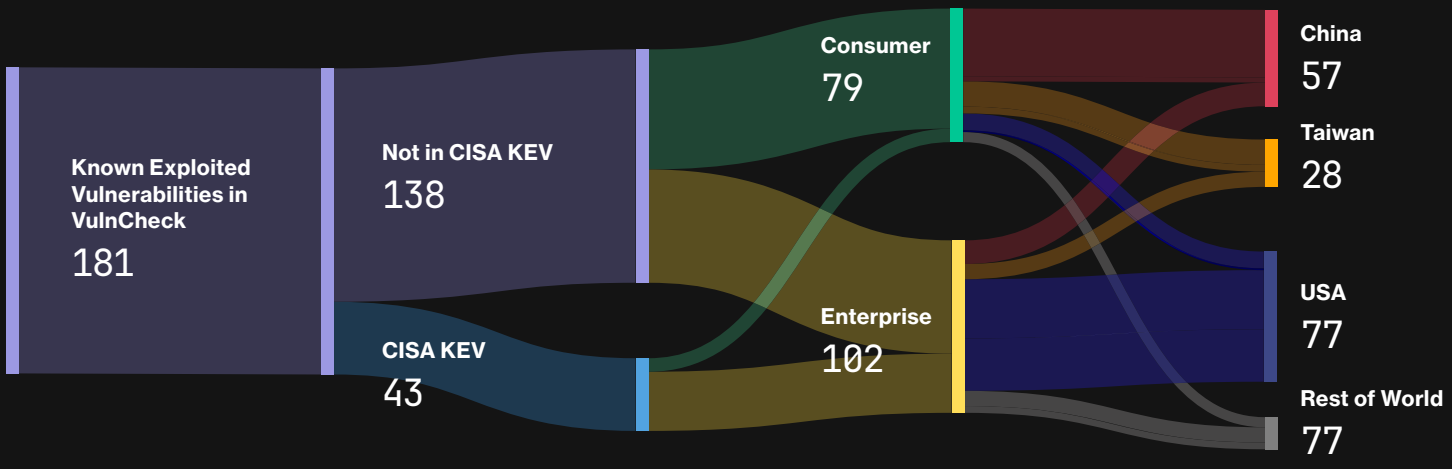
This suggests that both CISA KEV and the broader exploitation evidence tracked in VulnCheck KEV provide meaningful visibility into the risks posed by EOL network edge devices across enterprise, remote work, and global presence.

EOL Status of Network Edge Devices: CISA KEV



# Vendor Geography and Exploitation Visibility

Network Edge Device Vulnerabilities added to VulnCheck KEV in 2025




Another area we were interested in exploring was the relationship between exploited technologies and the geographic location of a vendor's headquarters, rather than where the products are manufactured.

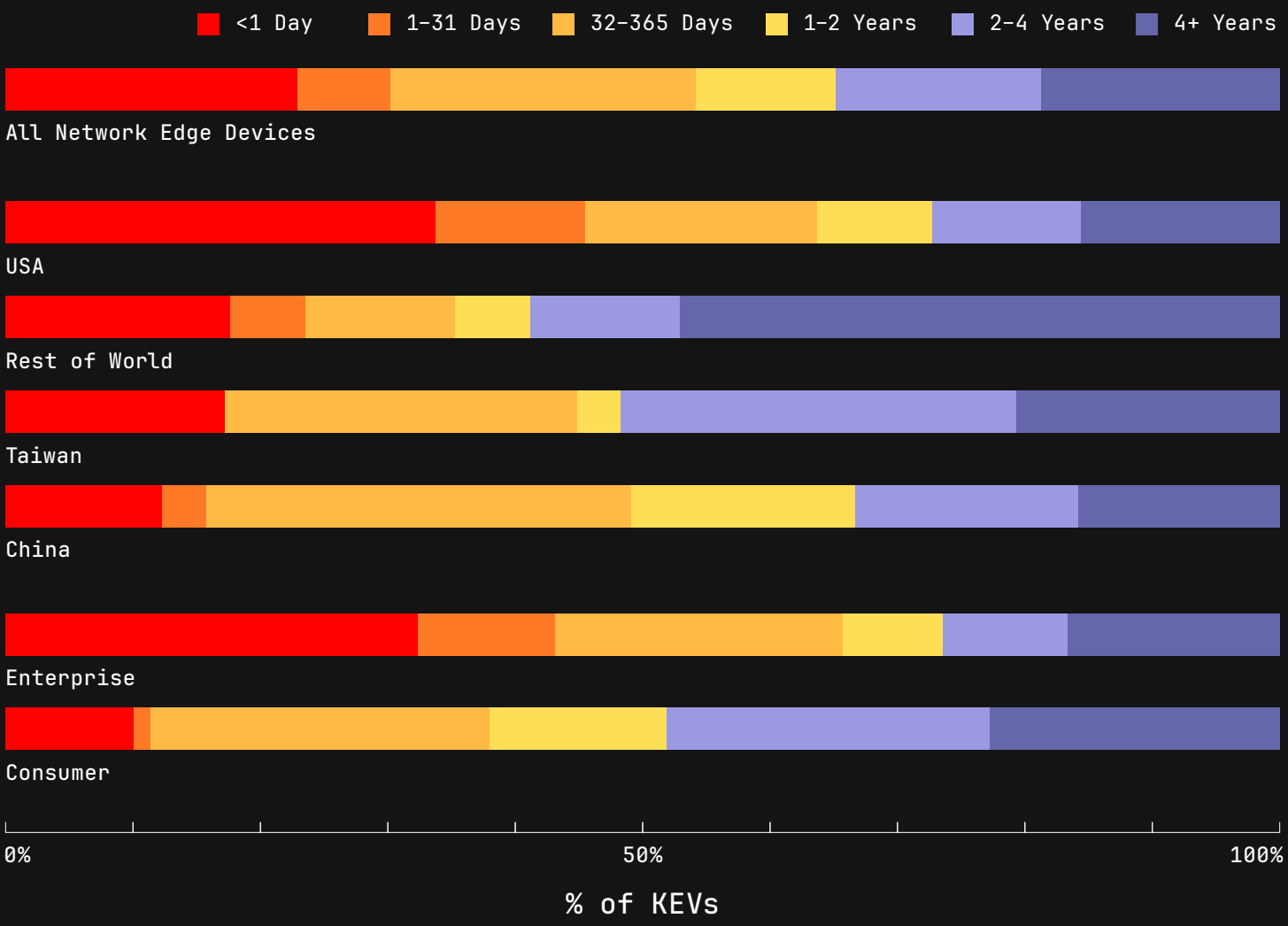
An interesting pattern emerged when comparing consumer and enterprise technologies. Consumer devices that are frequently exploited, particularly those leveraged by botnets, often originate from vendors headquartered in China. In contrast, many enterprise products observed being exploited tend to come from companies headquartered in the United States.

Many consumer devices targeted by botnets originate from inexpensive, mass-market products produced by Chinese vendors. These products often receive limited long-term software support, including infrequent security updates and minimal public vulnerability disclosure processes. As a result, vulnerabilities affecting these devices are often identified and disclosed by independent security researchers or third parties rather than the vendors themselves.

Exploitation activity involving these devices may also be underreported. Limited transparency around vulnerability disclosure practices, differences in regulatory environments, and the absence of consistent reporting channels may all reduce visibility into the full scope of exploitation affecting these products.

# Edge Device Exploitation Timelines

We examined why the higher volume of KEVs in edge devices appears to have a slower timeline before exploitation evidence compared to other product categories we identified in the 2026 State of Exploitation report. To explore this, we looked at two angles: the country where the network edge device vendor is headquartered and the difference in exploitation timelines between consumer and enterprise devices.




What appears to be a slower exploitation timeline for Chinese and consumer devices is more likely a reflection of limited detection capabilities and a lack of public disclosure by manufacturers. In many cases, Chinese companies do not publicly disclose vulnerabilities in their products.

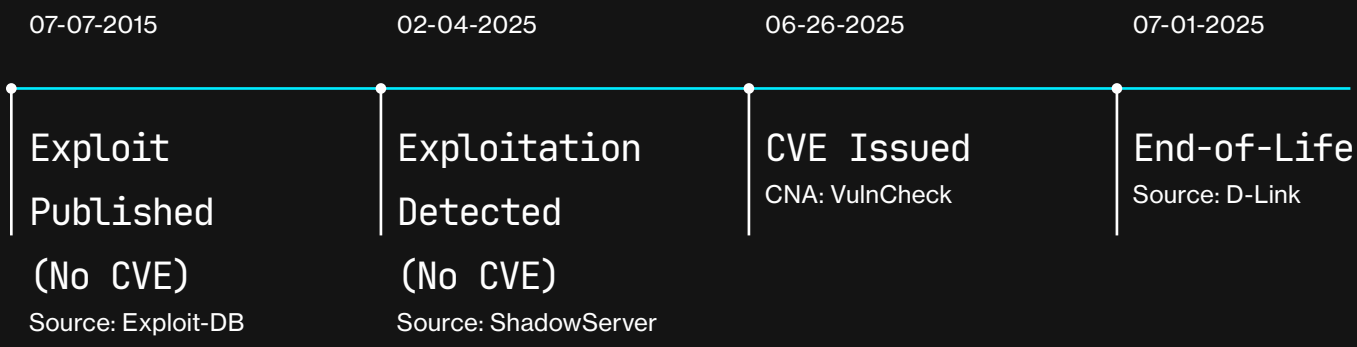
We have also frequently experienced manufacturers being unresponsive when we attempt to report vulnerabilities that are actively being exploited in the wild, leaving disclosure dependent on security researchers.

# VulnCheck CVE Assignments

Of the 181 network device KEVs included in this research, VulnCheck issued CVEs for 18 of them. These were discovered through exploitation evidence collected from VulnCheck Canaries and Shadowserver honeypots. In many cases, these vulnerabilities are identified for the first time by capturing exploit payloads being used in the wild.

## VulnCheck Exploited Vulnerability Timeline

CVE-2025-34048 | D-Link DSL-2750U

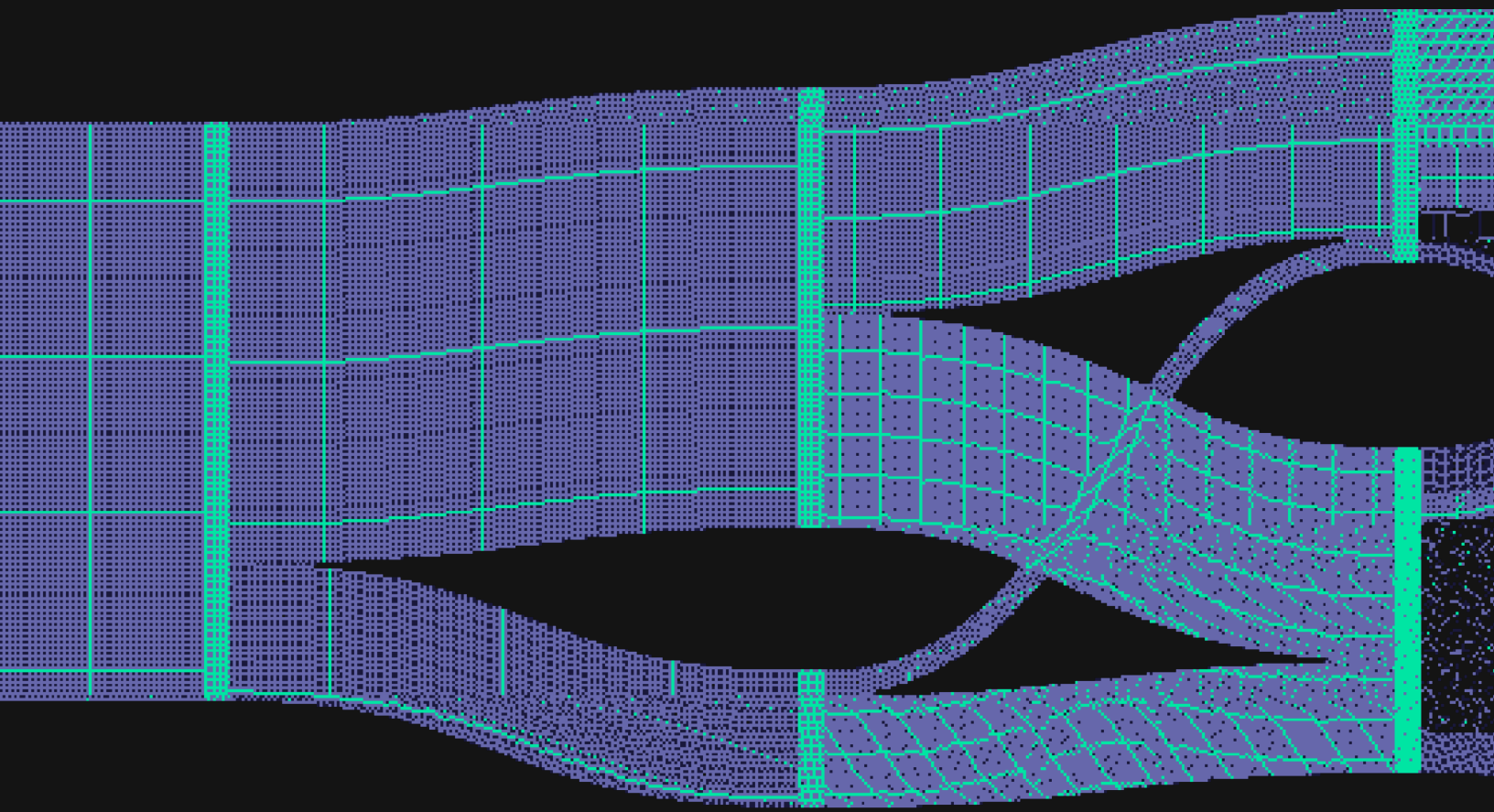



CVE-2025-34048, a vulnerability in the D-Link DSL-2750U, provides insight into some of the research VulnCheck is conducting to ensure CVEs are assigned to vulnerabilities in network edge devices that have public exploit code, exploitation evidence, and,in this case,affect an end of life product. In June, VulnCheck began working closely with Shadowserver to assign CVEs to actively exploited vulnerabilities that do not have one. Since then, we have expanded our CVE issuance and audit efforts to include sources such as Exploit-DB and other repositories where public vulnerabilities exist without an assigned CVE.

# End-of-Life Categorizations

During this research, we did our best to determine whether a product was end of life, end of sale, or still supported. End of life information is inconsistent across vendors and in some cases unavailable, so we used the following general methodology to determine whether the impacted product was supported, end of life, likely end of life, or end of sale.

| | |
|---|---|
| **End of Life (EOL)** | Marked as end of life by the software supplier or no updates to the product in five or more years. |
| **Likely End of Life** | No firmware or software updates in two or more years. |
| **End of Sale (EOS)** | The software supplier has stopped selling the product. |
| **Supported** | The software supplier marks the product as supported or has released updates within the past two years. |



# Advice for Enterprise Security Teams

Exploitation activity extends beyond the traditional enterprise, particularly through unsupported edge devices and widely deployed consumer networking equipment. Work from home devices and internationally distributed products are broadly targeted by exploitation activities that fall outside the scope of the US federal enterprise and CISA KEV. Use sources like VulnCheck to extend beyond the US federal ecosystem.

Efforts to reduce attack surface should include modernizing technology and removing end-of-life devices that continue to be targeted long after vendors stop supporting them.

Organizations should also evaluate the security posture of vendors whose products are deployed at the network edge. Vendors should clearly disclose vulnerabilities, publish end of life timelines, and communicate exploitation risks to customers. It is important to confirm that all vendors disclose vulnerabilities, report exploitation activity, and publish clear and current end of life information.

**Patrick Garrity** is a security researcher at VulnCheck where he focuses on vulnerabilities, vulnerability exploitation and threat actors.

## The VulnCheck Community

Explore the leading resource for open vulnerability and exploit intelligence:

- VulnCheck KEV
- NVD++
- VulnCheck Exploit Database (XDB)

**Join the Community →**

VulnCheck