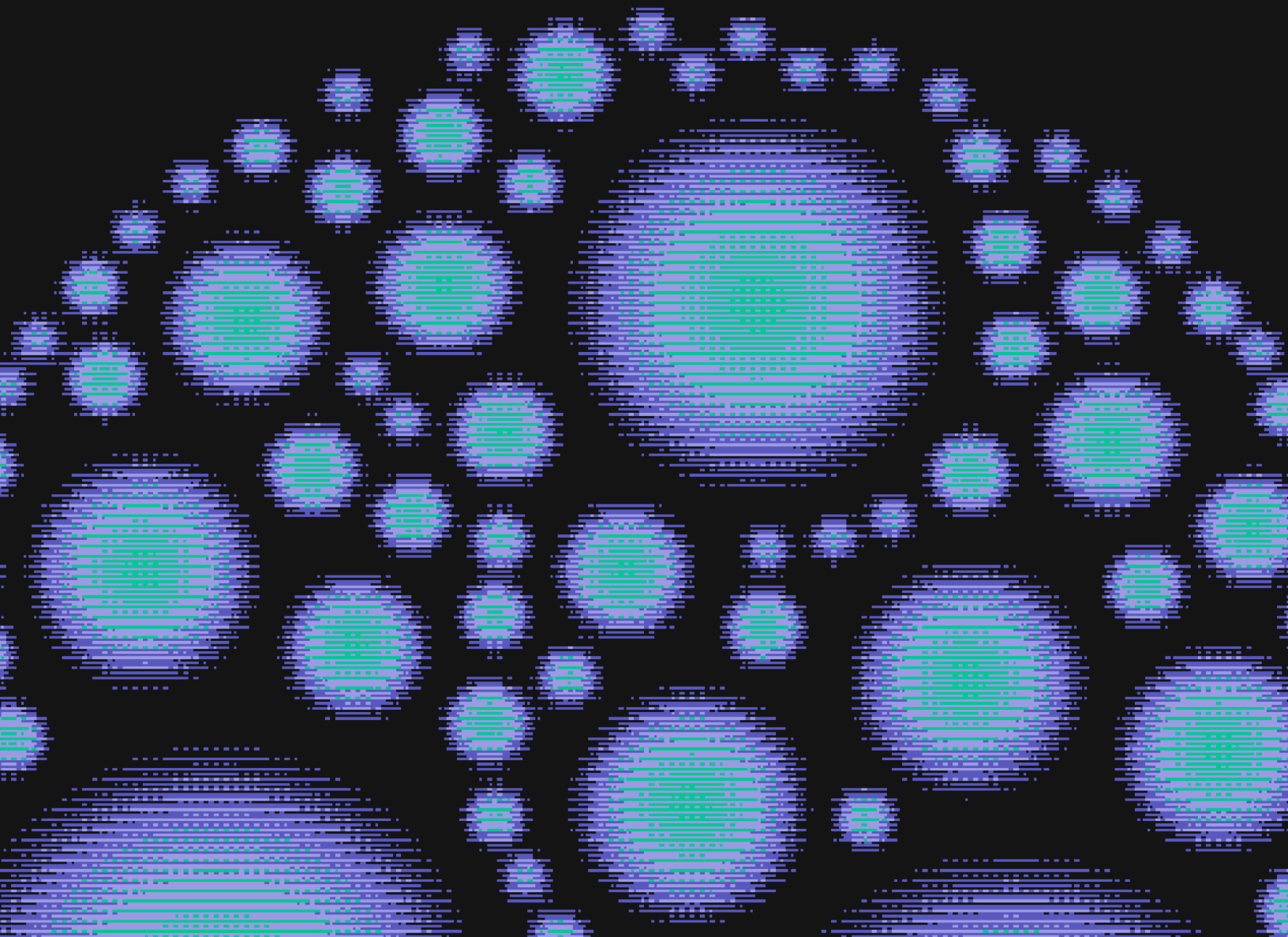
VulnCheck

State of Exploitation

2026

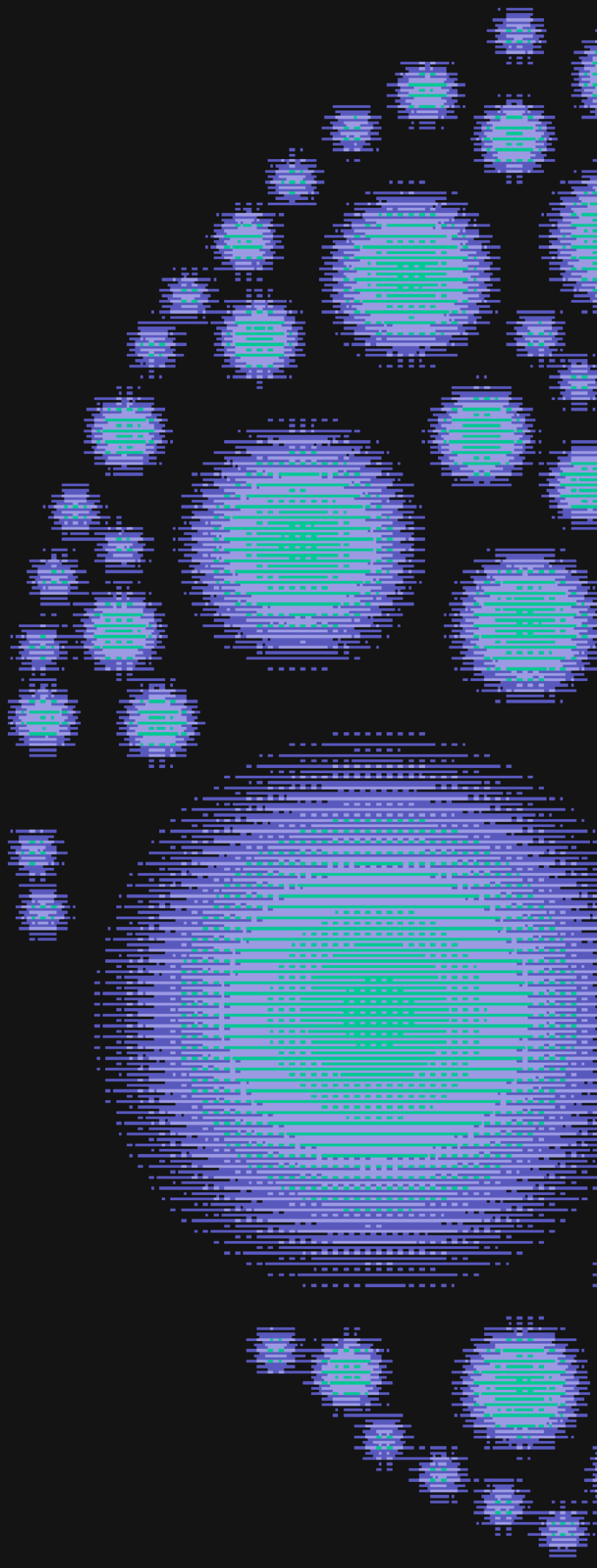


In 2025,

VulnCheck identified 884 Known Exploited Vulnerabilities (KEVs) for which evidence of exploitation was observed for the first time. By using the CVE publication date as a proxy for when defenders often gain awareness of a vulnerability, we can better understand how quickly exploitation follows disclosure and awareness. Our analysis shows that 28.96% of KEVs in 2025 were exploited on or before the day their CVE was published, an increase from the 23.6% observed in our 2024 trends in exploitation report, highlighting the continued prevalence of both zero-day[1] and n-day exploitation. This reinforces the urgency for organizations to act quickly on newly disclosed vulnerabilities while continuing to reduce long-standing vulnerability backlogs.

Throughout 2025, exploitation evidence was first reported by over 100 unique organizations, including security researchers, cybersecurity vendors, and software suppliers. Attackers continued to focus on internet-facing and widely deployed technologies, while also opportunistically exploiting a long tail of enterprise software, hardware, and emerging technology such as AI.

These trends demonstrate that exploitation speed remains consistently high year over year, and that defenders must prioritize visibility into exploited vulnerabilities with timely remediation in order to keep pace with attackers.



Key Takeaways

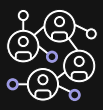
From VulnCheck's Analysis of KEVs in 2025

884 KEVs were identified with first-time exploitation evidence during 2025 and added to VulnCheck KEV.

Exploitation activity spanned hundreds of vendors and products, reflecting a broader coverage of enterprise technologies than is represented in public KEV catalogs alone.

28.96% of KEVs showed evidence of exploitation on or before the day the CVE was published, underscoring the persistence of rapid exploitation.

VulnCheck identified exploitation evidence for KEVs significantly earlier than CISA KEV in the majority of cases, often by days, months, or even years.



118 unique sources were first to publicly report exploitation activity, with hundreds more contributing corroborating evidence across the ecosystem.

Ransomware attribution continued to lag behind initial exploitation disclosure, suggesting that attribution for vulnerabilities exploited in 2025 will continue to grow as additional research is published.

Network edge devices, including firewalls, VPNs, and proxies, were the most frequently targeted technologies, followed by content management systems and open source software.

Time-to-exploitation patterns in 2025 remained highly consistent with 2024, indicating stable and sustained attacker behavior.

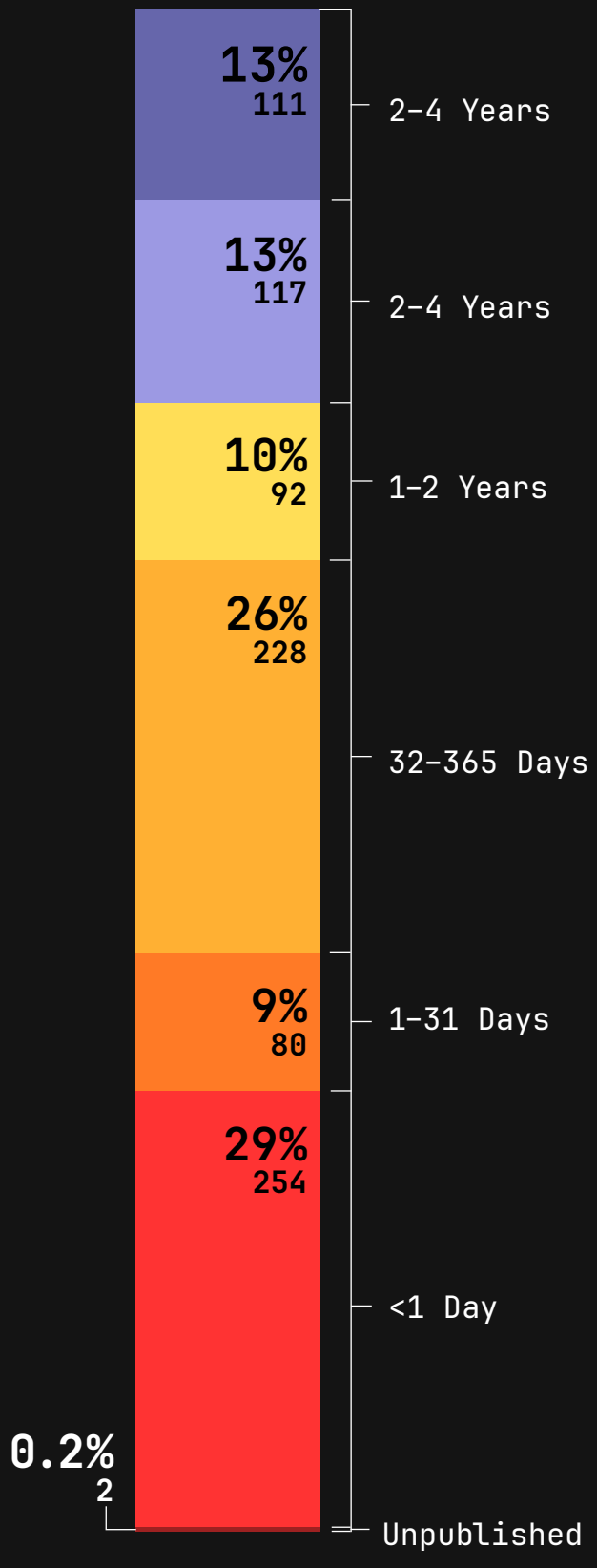
This research was completed using VulnCheck KEV which is available as a free community service. During 2025 we expanded VulnCheck KEV to include E-mail and Slack alerting.

KEV Exploitation Timeline

2025

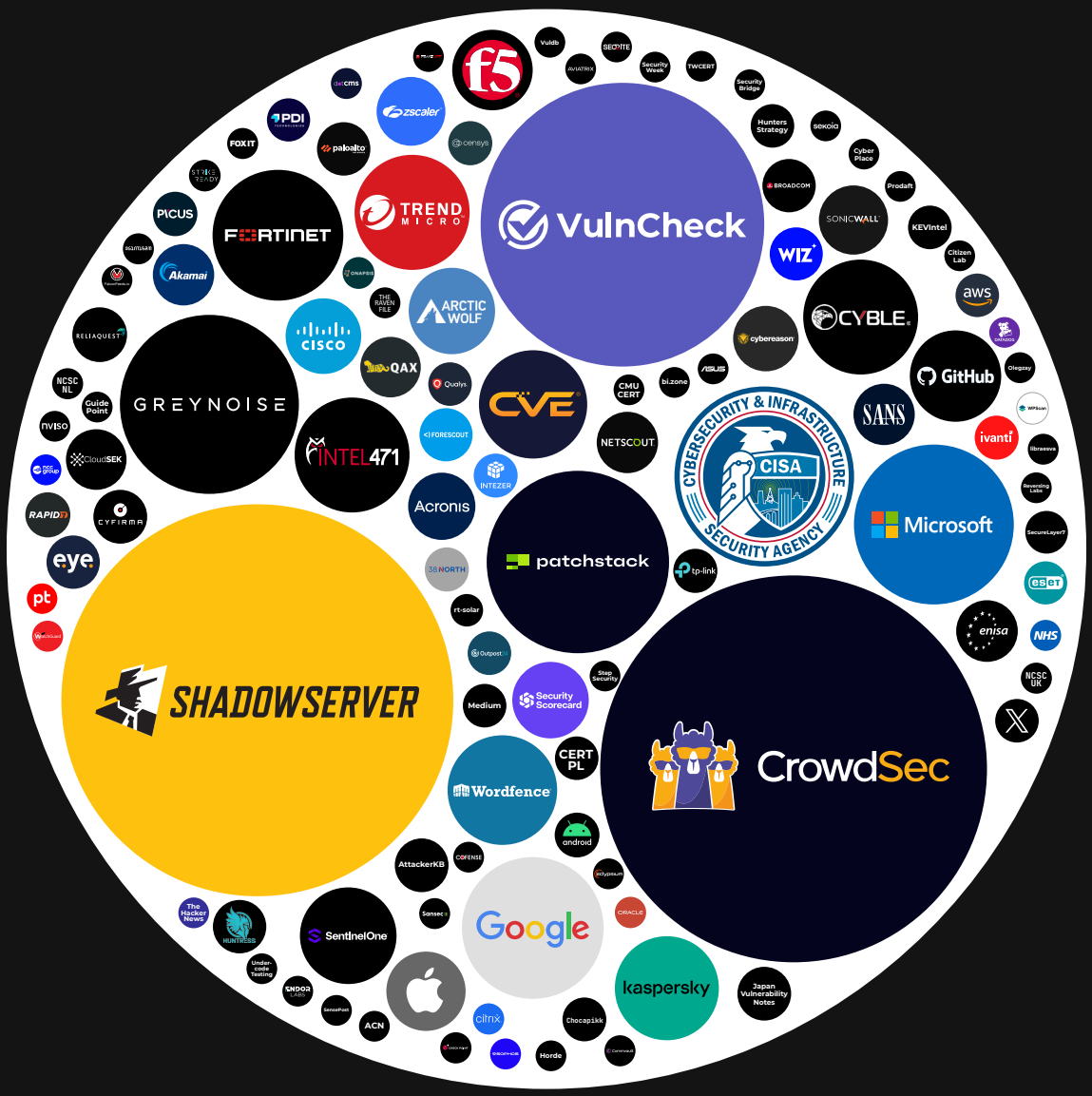
During 2025, VulnCheck identified exploitation activity for 884 Known Exploited Vulnerabilities (KEVs) that had no evidence of exploitation prior to 2025. To better understand how quickly vulnerabilities are exploited, we use the CVE publication date as a reference point for when defenders typically first gain visibility into a vulnerability.

Our analysis shows that 28.96% of the KEVs identified in 2025 were exploited on or before the day their CVE was published, underscoring the speed at which threat actors operate and often exploit vulnerabilities, often before public disclosure or CVE issuance occurs. This highlights the need for vulnerabilities early in their lifecycle are addressed when exploitation risk is high, while continuing to remediate older vulnerabilities that persist.



First Reporter of Exploitation

2025

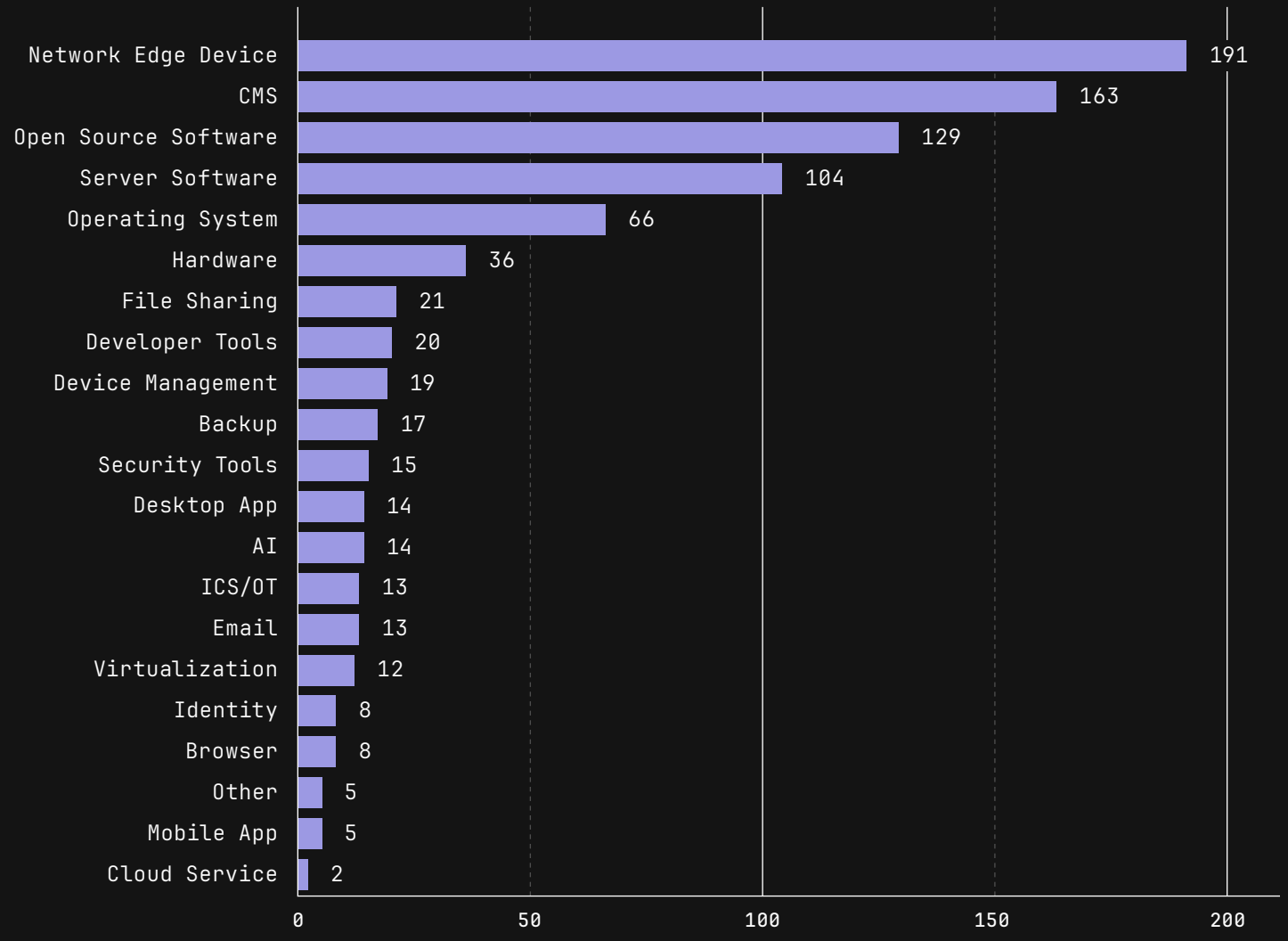


By analyzing source-level evidence of exploitation, we identified which organizations publicly disclosed exploitation evidence first. In 2025, we observed 118 unique sources that were the first reporters of exploitation activity, with hundreds of additional sources contributing corroborating evidence.

Transparency in exploitation disclosure is critical, as it enables consumers to better understand who first reported exploitation and to assess the level of trust they place in each source. Shadowserver remained the leading source for first-to-report exploitation evidence.

The most notable increases in sources that were first to report KEVs included CrowdSec, which was onboarded as a new source and scaled significantly in 2025, and VulnCheck, following the launch of VulnCheck Canary Intelligence.

Top Targeted Technologies



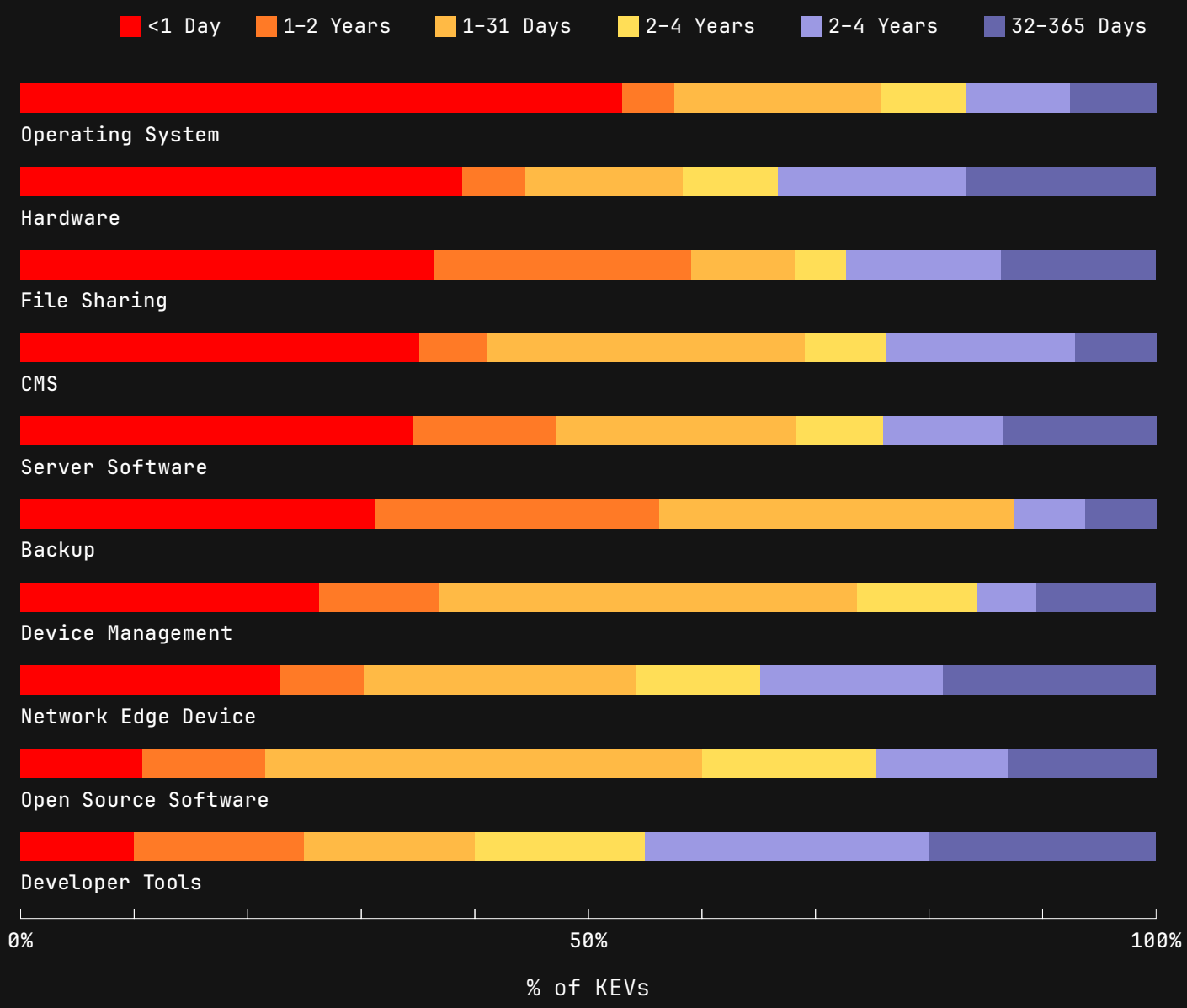
Looking at the top technologies being targeted, network edge devices such as firewalls, VPNs, and proxies top the list. This is not surprising, as they are internet-facing devices that often serve as a jumping-off point into an enterprise environment or home network. Content management systems, largely dominated by the WordPress ecosystem, are also frequent targets because they are commonly exposed to the internet.

Open source software ranked third in 2025, followed by server software and operating systems such as Microsoft Windows, Linux, Apple, and Android.

However, exploitation spans a broad range of enterprise technologies and extends beyond these categories to include hardware devices, most often camera systems, as well as file sharing platforms, developer tools, device management systems, backup solutions, security tools, desktop applications, AI systems, ICS and OT environments, email platforms, virtualization technologies, identity systems, browsers, mobile applications, cloud services, and more. Threat actors are opportunistic, leveraging both older, well-known vulnerabilities and newly disclosed flaws to access systems and establish footholds across the enterprise.

Top Targeted Technologies

Time from CVE to Exploitation Evidence



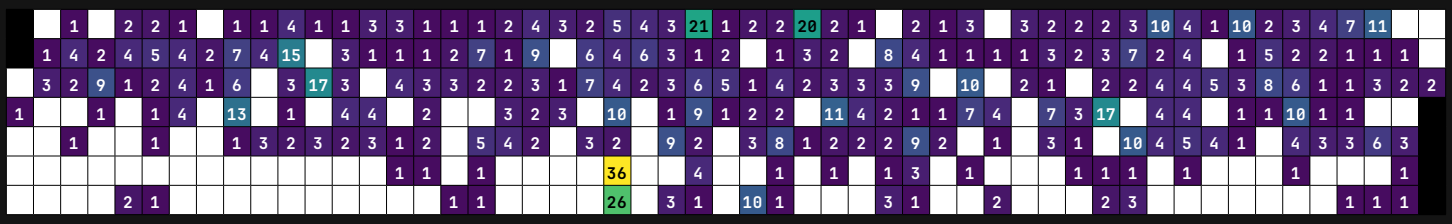
Breaking out the top ten targeted technologies and examining exploitation timelines relative to CVE issuance provides additional insight into the relationship between exploitation and disclosure.

Operating systems top the chart, likely because vendors such as Microsoft, Apple, and Android frequently disclose evidence of exploitation alongside their security advisories.

This year, we spent considerable time issuing CVEs targeting camera systems, which fall under the hardware category. This likely reflects the relative immaturity of vulnerability disclosure and issuance practices among hardware manufacturers. While each category could warrant its own dedicated research project, this analysis provides defenders with a clearer sense of how quickly they need to prioritize patching for each technology.

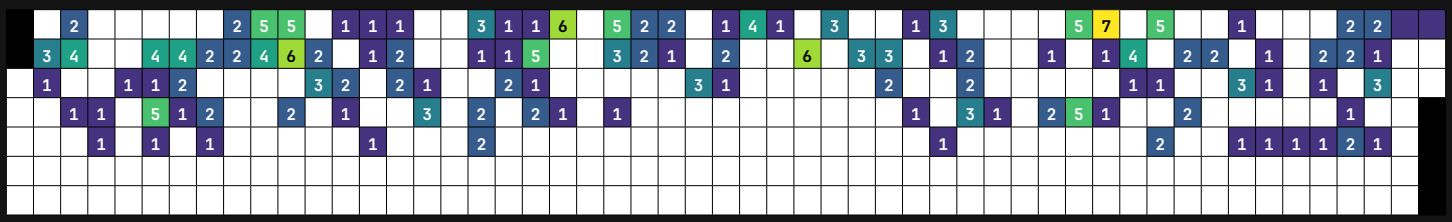
VulnCheck KEV vs. CISA KEV

VulnCheck KEV

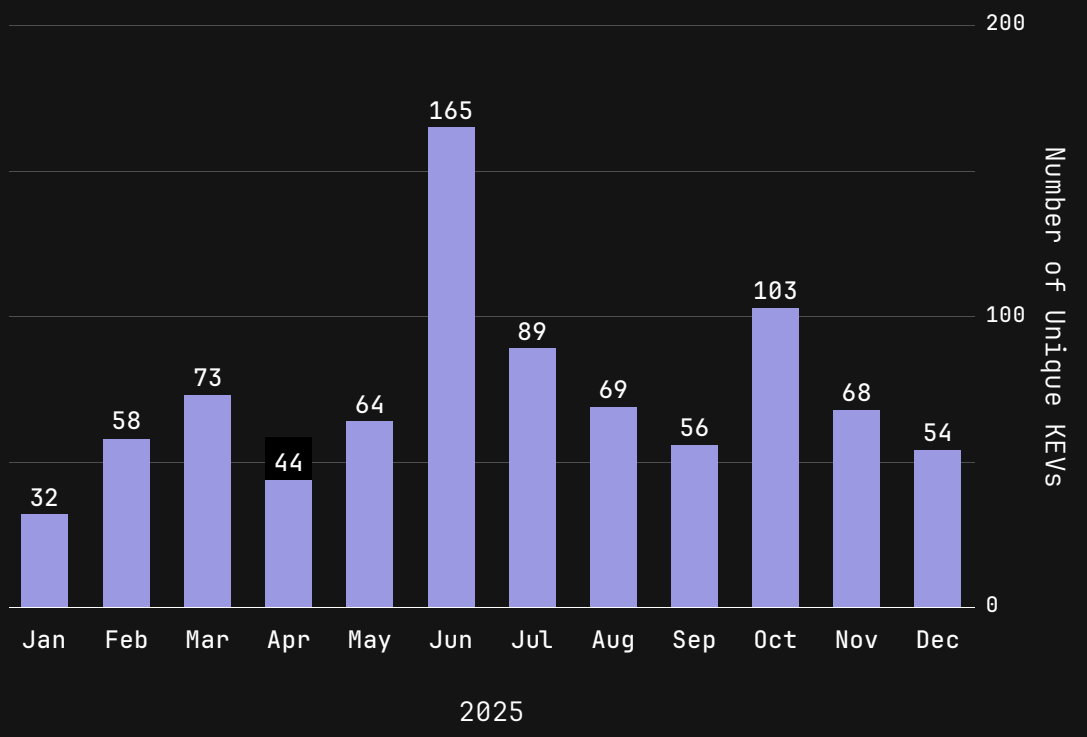


JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC

CISA KEV



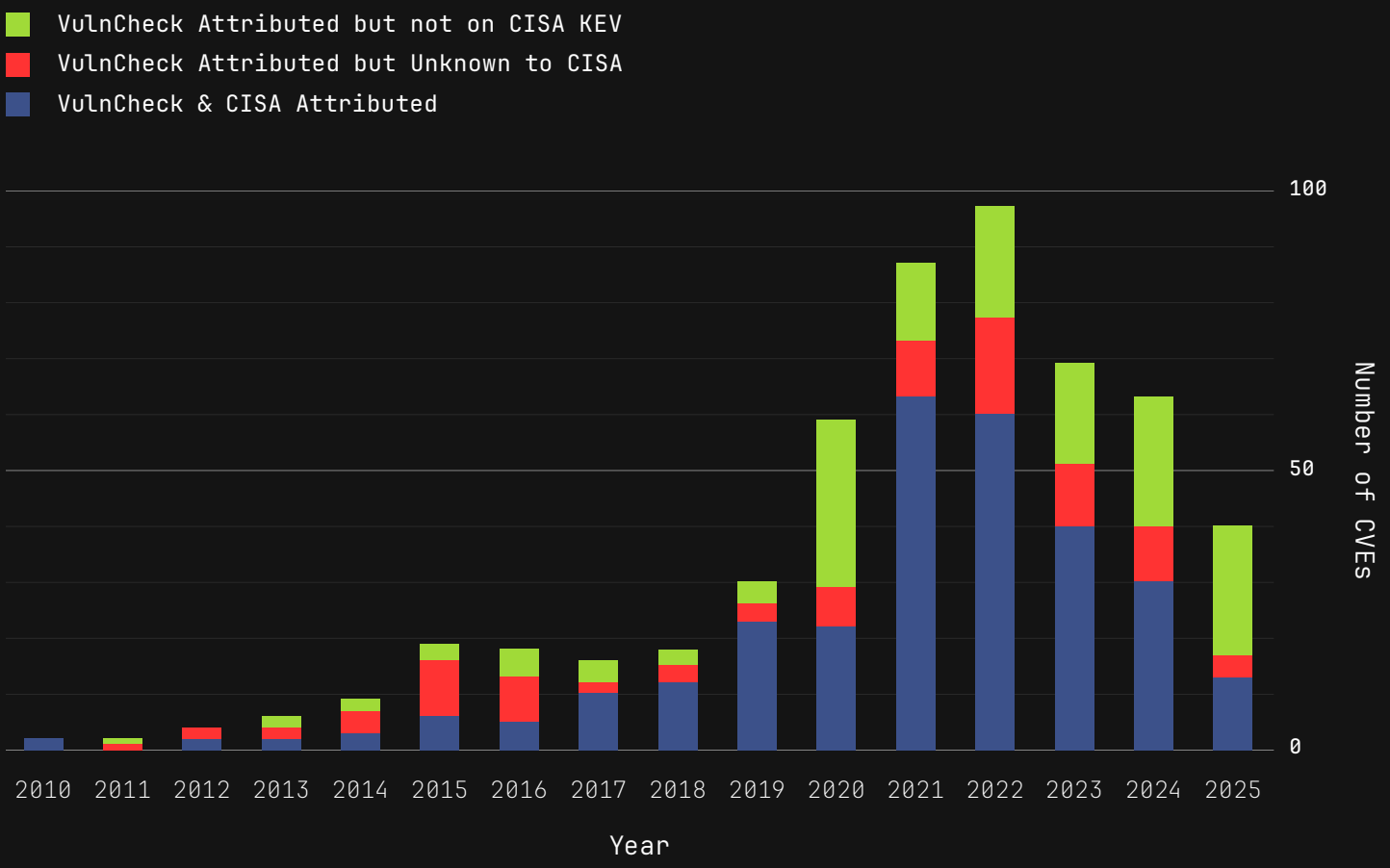
During the year, VulnCheck identified 884 unique KEVs across 518 vendors and 672 products, while CISA added 245 KEVs across 99 vendors and 146 products, most of which are high impact and pervasive across the federal landscape. One of the biggest differences is the volume of vendors and projects covered. Additionally, VulnCheck added evidence to its KEVs more than 85 percent of the time, often predating CISA by days, months, or even years.



Exploitation of Real Vulnerable Hosts Not on CISA KEV

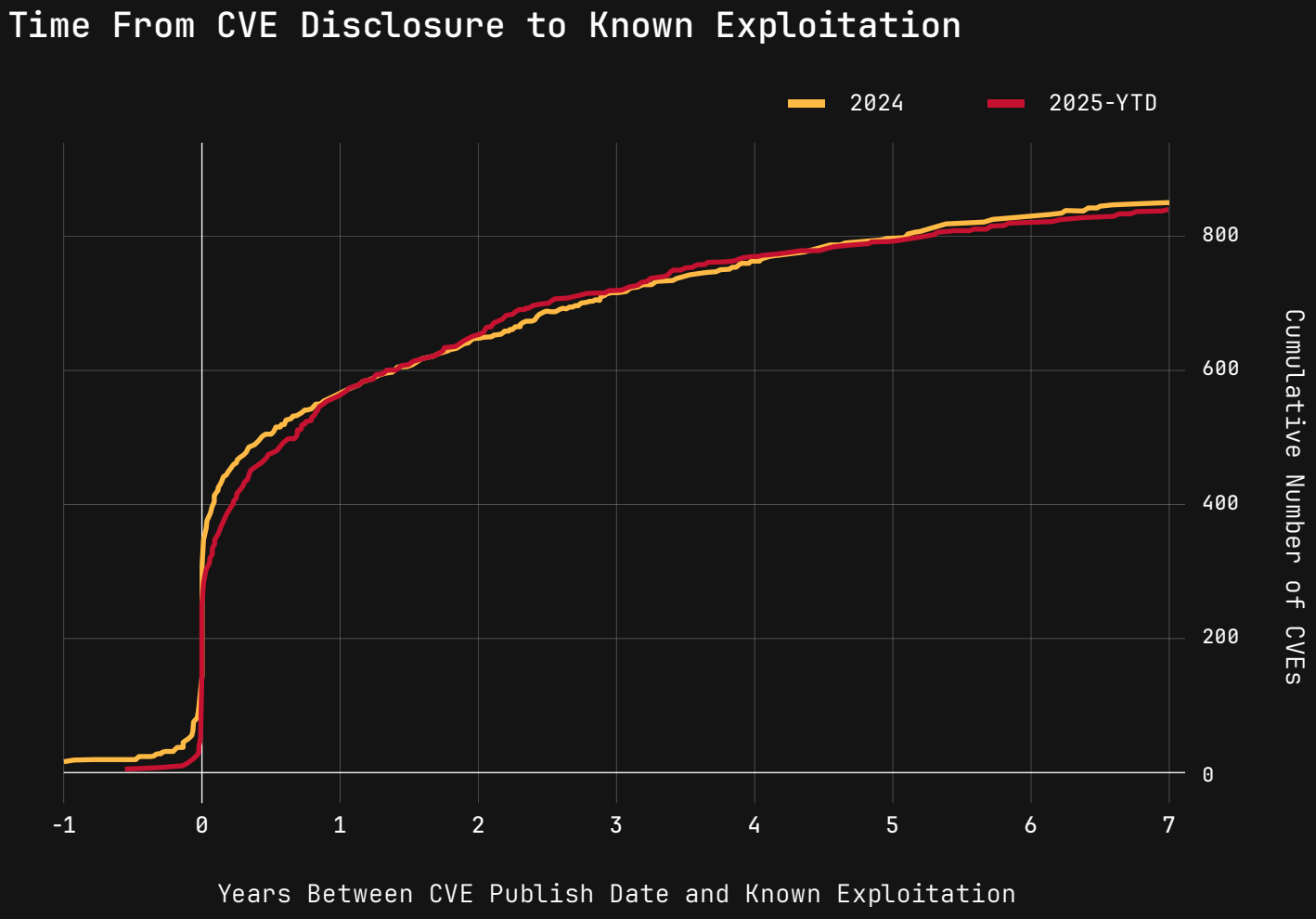
In October 2025, we added exploitation indicators to VulnCheck KEV sourced from VulnCheck's Canary Intelligence service. When exploitation of a vulnerability is detected against a real vulnerable host that we have deployed, an indicator is added to VulnCheck KEV. This provides valuable insight into technologies where exploitation has been observed on real-world systems, but the vulnerabilities are not listed in CISA KEV.

Ransomware Attribution Over Time



The spike observed in 2021 and 2022 is likely a direct result of the initial release of CISA's Known Exploited Vulnerabilities (KEV) catalog, which included early additions and associated ransomware attribution. We are now likely seeing stabilization in the number of vulnerabilities used in ransomware campaigns. However, because ransomware attribution is often delayed relative to initial exploitation disclosures, we expect attribution for vulnerabilities known to be exploited in 2025 to continue increasing as additional research is published.

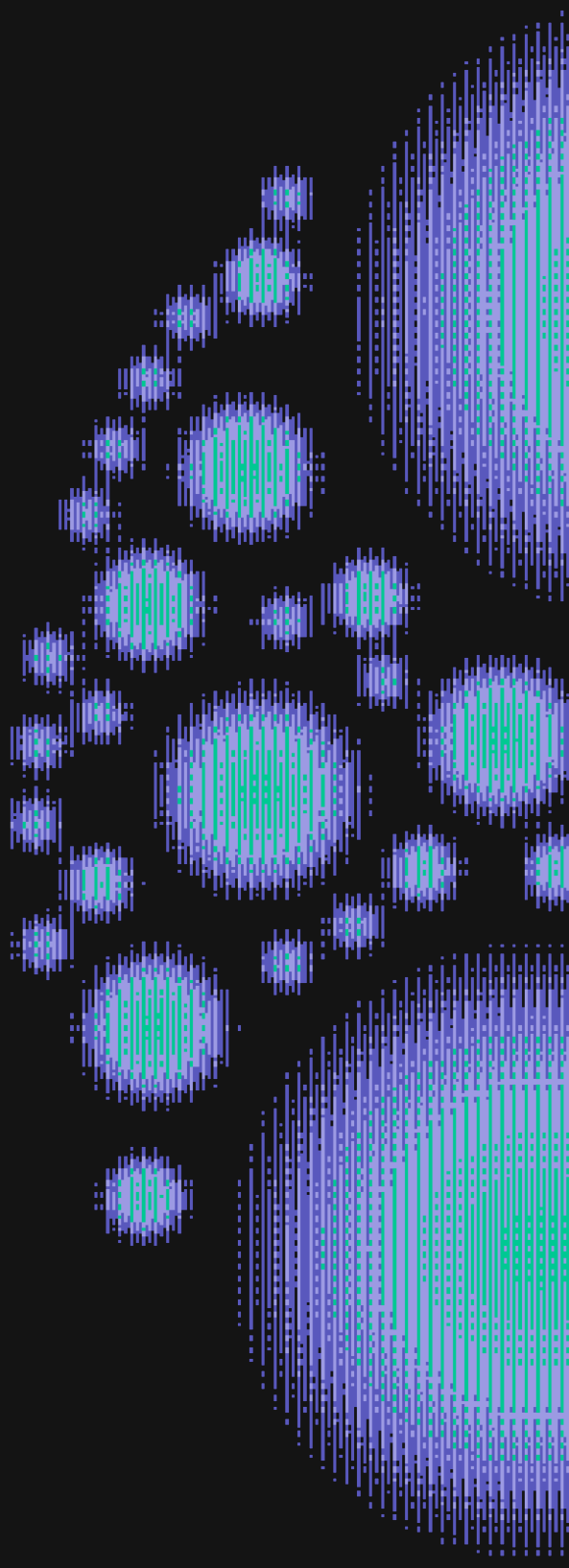
Exploitation Timeline 2024 vs. 2025



Time to exploitation remained highly consistent between 2024 and 2025, with only minor deviations, indicating consistent exploitation activity in known exploited vulnerabilities across both years.

Summary

2025 reinforces the reality that exploitation speed remains a defining challenge for defenders. With nearly 900 KEVs first observed as exploited during the year, sustained prevalence of zero-day and n-day exploitation activity, and continued targeting of internet-facing and widely deployed enterprise technologies, organizations face little margin for delayed response. While time-to-exploitation patterns remained consistent with 2024, the scale and breadth of affected vendors, products, and technologies continue to expand. Maintaining strong vulnerability management practices, prioritizing trusted exploitation intelligence, and monitoring beyond the CISA KEV catalog remain critical to reducing exposure and staying ahead of adversaries.



Considerations For This Report

- Not all KEVs being exploited on the same day of CVE issuance are Zero Days.
- The CVE for 81 of the KEVs that were identified as being exploited in the wild during 2025 were published by VulnCheck through the VulnCheck research team, partnership with ShadowServer, and from our report a vulnerability service.

The VulnCheck Community

Explore the leading resource for open vulnerability and exploit intelligence:

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

VulnCheck

Join the Community →