secpod

Q2 Vulnerability Report

www.secpod.com

Executive Summary

Unified Security Intelligence as a Strategic Enabler of Continuous Vulnerability and Exposure Management.

The Q2 threat landscape reveals a clear escalation in enterprise risk: a 15% rise in total vulnerabilities, with a disproportionate 13% marked as critical or high severity. These figures highlight a growing attacker advantage and shrinking time-to-exploit.

In this context, Unified Security Intelligence (USI) has become a strategic imperative. USI consolidates vulnerability intelligence, exploit data, misconfiguration data, and patch controls into a unified operational layer. This enables continuous visibility, real-time prioritization, and measurable risk reduction across infrastructure, on-prem, cloud, and hybrid. With over 5,700 CVEs tracked, including 16 zero-days, 40+ CISA KEVs, and 1,600+ mapped remediations, USI ensures no critical exposure is left behind.

Where traditional tools operate in silos, USI provides a single source of truth that aligns with business risk. It enables security leaders to:

- Quantify and communicate exposure: From kernel-level exploits to application-layer vulnerabilities in Adobe, VMware, and Microsoft.
- Enforce consistent controls: Through CRE and CCE-mapped remediation, across Windows, Linux, and macOS platforms.
- Accelerate MTTR: By automatically prioritizing patching based on exploitability, asset criticality, and relevance.

Importantly, USI empowers the shift from episodic scans to continuous vulnerability and exposure management (CVEM).

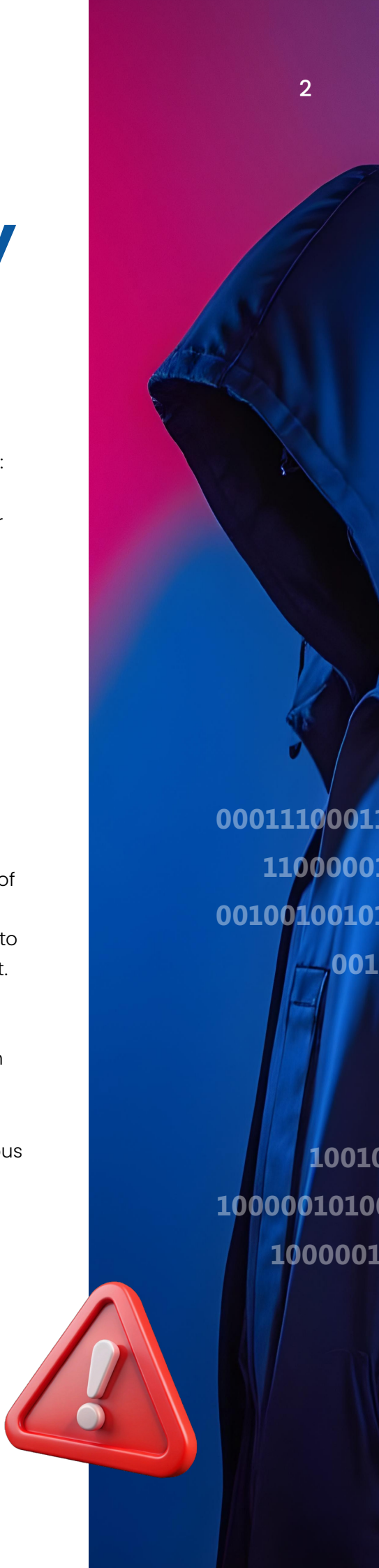


Table of Contents

Q2 Key Highlights & Trends

Here are some of the most significant vulnerability trends observed this quarter.

15% rise in vulnerability when compared to Q1. The 10,510 findings reflect how vulnerabilities can increase due to a lack of unified security intelligence.

13% rise in vulnerabilities that are either critical or high severity. This unequal share poses immediate business risks.

40 widely exploited vulnerabilities highlight attackers' agility in weaponizing known flaws.

94 Malware Vulnerability Enumerations with high impact exploitability are also part of widely exploitable vulnerabilities.

Q2 Report Coverage

The data demonstrates how USI can consolidate various security checks into a single source of truth. This helps in prioritizing high-risk weaknesses (zero days, CISA KEVs), balancing host and network-level insights, and ensuring both vulnerabilities and misconfigurations are managed under one roof.

CVEs Covered: 5711

SecPod's USI can ingest and correlate various vulnerabilities, ensuring no common CVE is missed.

Local Checks 6339 vs. Remote Checks: 395

There's a strong emphasis on host visibility (configuration, patch level, registry, file integrity), while external attack surface scans remain relatively lighter. This emphasizes the importance of improving perimeter and SaaS assessments.

Zero Days Covered: 16

By ingesting and tagging zero-day intelligence, USI shows that critical exposures are flagged immediately for faster containment before public exploit kits emerge.

CISA Vulnerability Coverage: 40

Automatic mapping of your IT environment against CISA's Known Exploited Vulnerabilities list means you stay compliant with U.S. federal mandates and can prove due diligence during audits.

Network Device Vulnerabilities: 1015

USI's ability to profile and score network devices (routers, switches, firewalls) ensures unified risk visibility across device and network layers.

Misconfigurations & CCEs Covered: 959

Uniformity between misconfiguration findings and CCEs shows USI's tight integration with configuration controls, which ensures that every deviation is turned into a standardized, actionable control.

The patching metrics below illustrate how USI ensures end-to-end remediation and visibility. Together, these figures underscore USI's role from detection to remediation, standardizing, prioritizing, and automating every security gap.

Comprehensive CRE Mapping (1,616 CREs):

USI automatically aligns each fix to the Common Remediation Enumeration standard, enabling consistent tracking and reporting across diverse Win, macOS and Linux environments.

Third-Party Application Coverage (559 Patches):

USI ingests vendor advisories and community feeds, bringing third-party application patch data into the same dashboard as OS updates, eliminating silos.

Configuration Remediation (795 Misconfiguration Patches):

USI treats misconfiguration fixes the same as software patches, including them in compliance workflows.

Unified Patch Orchestration (2,354 Total Patches):

With over 2,300 total patches managed, USI ensures automatic assigning, tracking, and verification of patch deployments across on-prem, cloud, and endpoint landscapes.

RISK INSIGHT

While the coverage and remediation numbers offer considerable control, the deeper insights in this Q2 report reveal where true risks are and why they demand continuous attention. The 15% quarter-on-quarter spike in vulnerabilities and the disproportionate share, 13% of critical and high-severity exposures, signal more than just volume. They point to increased attacker opportunity and reduced MTTR.

Along with 16 zero days this quarter, 47 widely exploited CVEs and 30 MVEs show that adversaries have more opportunities to exploit known weaknesses at scale.

Total Number of CVEs Covered

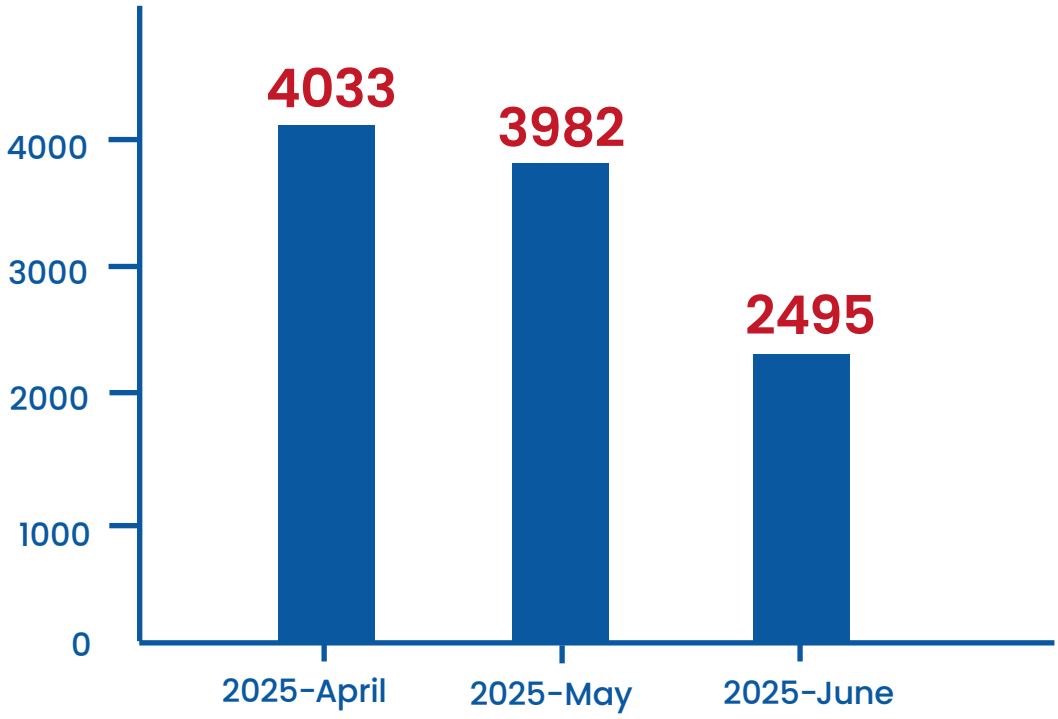


Figure 1: Shows the Number of vulnerabilities published from April to June 2025

In Q2, 5,711 CVEs were identified, but a closer look at monthly breakdown reveals an important story:

April: 4,033 vulnerabilities | May: 3,982 vulnerabilities | June: 2,495 vulnerabilities

This downward trend may appear encouraging at first glance, but from a Unified Security Intelligence (USI) perspective, it's a critical reminder that volume doesn't equate to lower risk. Even as vulnerability counts reduce, exploitability and business impact remain high, especially with more threats weaponizing known flaws. USI continuously ingests CVE data, maps it against your IT infrastructure, and applies threat context, ensuring that even as new disclosures change monthly, you remain focused on what's exploitable and urgent. In essence, USI helps turn raw CVE volume into prioritized, business-aware action, month after month.

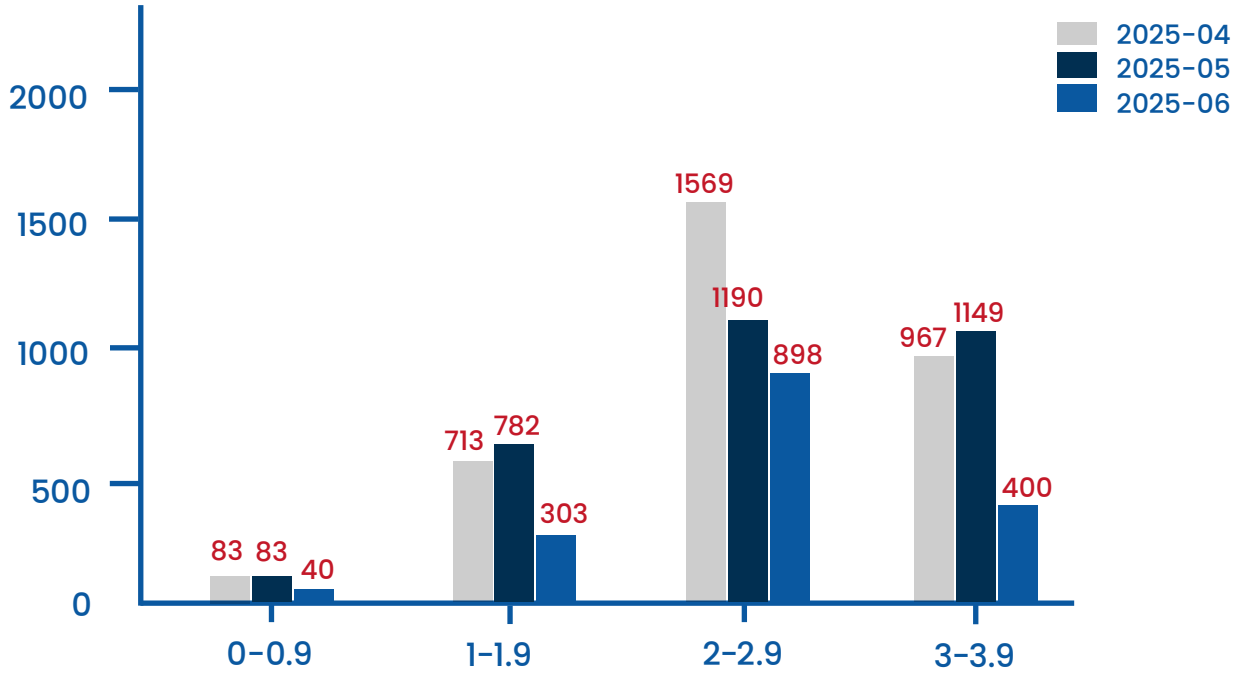
RISK INSIGHT

Continuous mapping of vulnerability exploitability and business impact is needed to ensure declining vulnerability volume never translates into reduced vigilance, keeping remediation efforts focused on weaknesses attackers are most likely to target.

Vulnerability exploit and impact distribution based on CVSS v3

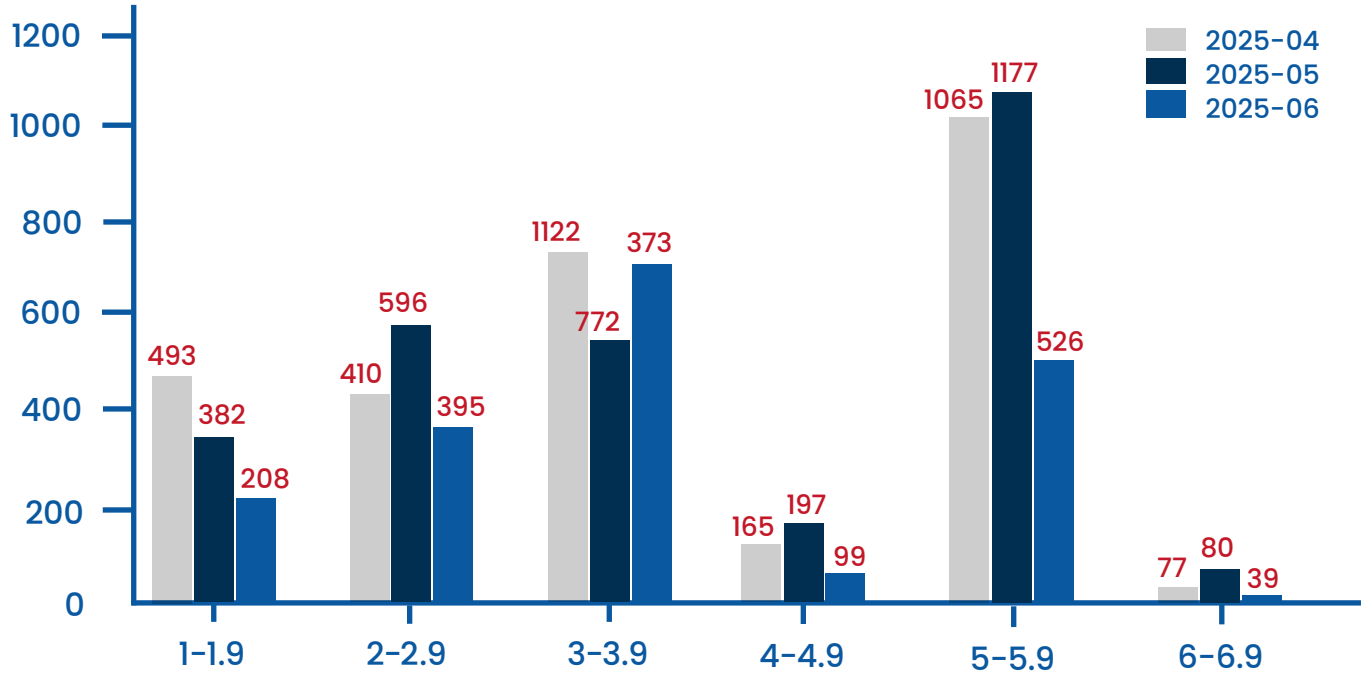
CVSSv3 EXPLOIT SUBSCORE DISTRIBUTION

Figure 2: Depicts the vulnerability exploit subscore distribution based on CVSSv3



CVSSv3 IMPACT SUBSCORE DISTRIBUTION

Figure 3: Depicts the vulnerability impact subscore distribution based on CVSSv3



Even as overall CVE counts dipped from April through June, the underlying risk profile remained quite high. Here are some key observations.

Exploitability stayed elevated
In April and May, most vulnerabilities clustered in the 2.0 to 2.9 and 3.0 to 3.9 exploitability ranges, where real-world weaponization is common. June saw lower totals, but nearly 1,300 CVEs still scored above 2.0, showing that adversaries have plenty of targets they can exploit.

Potential business impact climbed
April's impact scores already showed over 2,100 CVEs in the 3.0 to 3.9 and 5.0 to 5.9 range. May pushed that higher, with the 5.0 to 5.9 bucket topping 1,100. Even in June, more than 500 high-impact flaws remained.

RISK INSIGHT

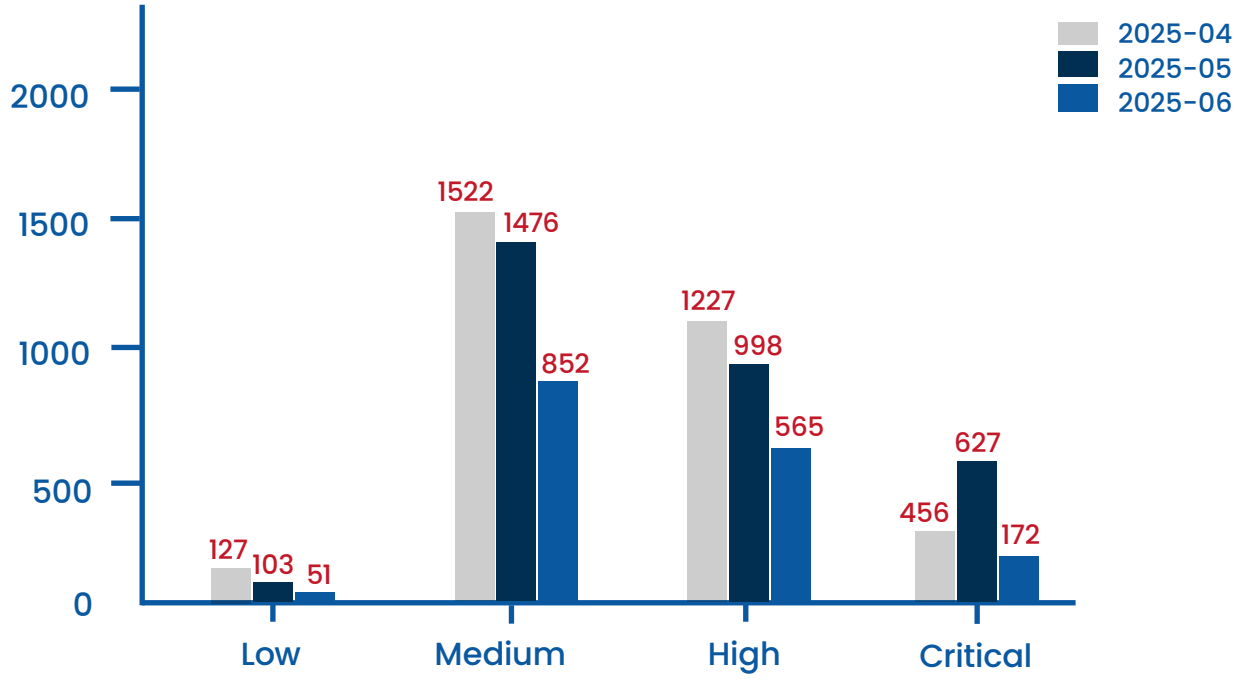
There is a stubborn core of high-exploitability and high-impact flaws, over 1,300 vulnerabilities with proven weaponization potential and more than 500 capable of severe business disruption linger even in June. Continuous, intelligence-driven risk prioritization is needed to neutralize these vulnerabilities most likely to be exploited and most damaging if breached.

Know more about risk prioritization.

Monthly CVSS V3 Distribution

MONTHLY CVSSv3 DISTRIBUTION

Figure 4: Depicts the vulnerability distribution monthly CVSS V3



USI does not only track vulnerability volume, it tracks how it evolves across time to track distribution trends. The chart illustrates how the balance of low, medium, high, and critical vulnerabilities has shifted across April, May, and June 2025:

- Critical vulnerabilities spiked in May, outpacing both April and June, a clear indicator that exploit-ready risks surged mid-quarter.
- High and medium severity vulnerabilities remain consistently elevated, making them key zones for patch prioritization.
- Low-severity issues declined steadily, indicating that attackers and security teams are focusing on higher-impact exposures

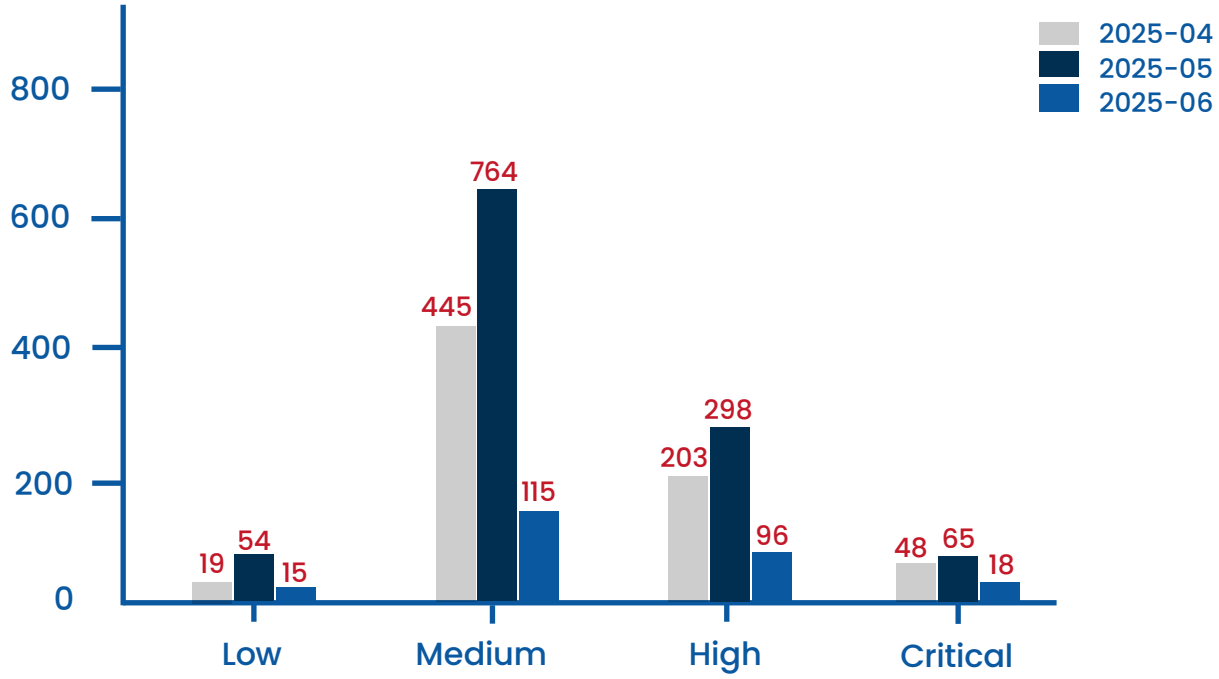
RISK INSIGHT

This pattern underscores the need for aggressive prioritization of critical and high-severity patches, continuous monitoring of severity trends and shift from volume-based to impact based remediation.

Monthly CVSS V4 Distribution

MONTHLY CVSSv4 DISTRIBUTION

Figure 5: Depicts the vulnerability distribution monthly CVSS V4



As Unified Security Intelligence evolves, so does the way we evaluate vulnerability risk. CVSSv4 offers a more nuanced model than CVSSv3, emphasizing exploitability, environmental context, and system impact, not just static scores. This chart reveals a telling trend:

- Medium-severity vulnerabilities dominate, making up the bulk of detected CVEs across all three months.
- Critical and high-severity vulnerabilities remain relatively low in count, but their operational risk remains high due to exploit potential.
- May saw the highest volume overall, indicating a spike that may correspond with heightened threat activity or vendor disclosure patterns.

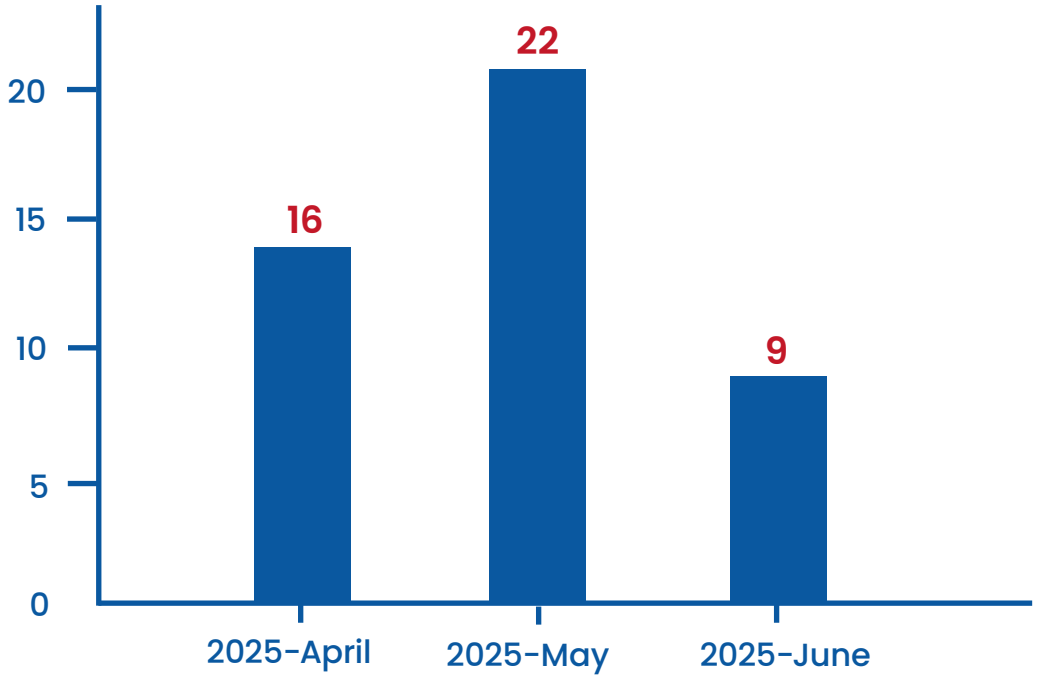
RISK INSIGHT

The CVSSv4 distribution shows a dominance of medium-severity vulnerabilities. Many of these “medium” issues may carry high exploitability in specific environments, especially when stacked with other weaknesses.

Total Number of widely exploited & high fidelity vulnerabilities

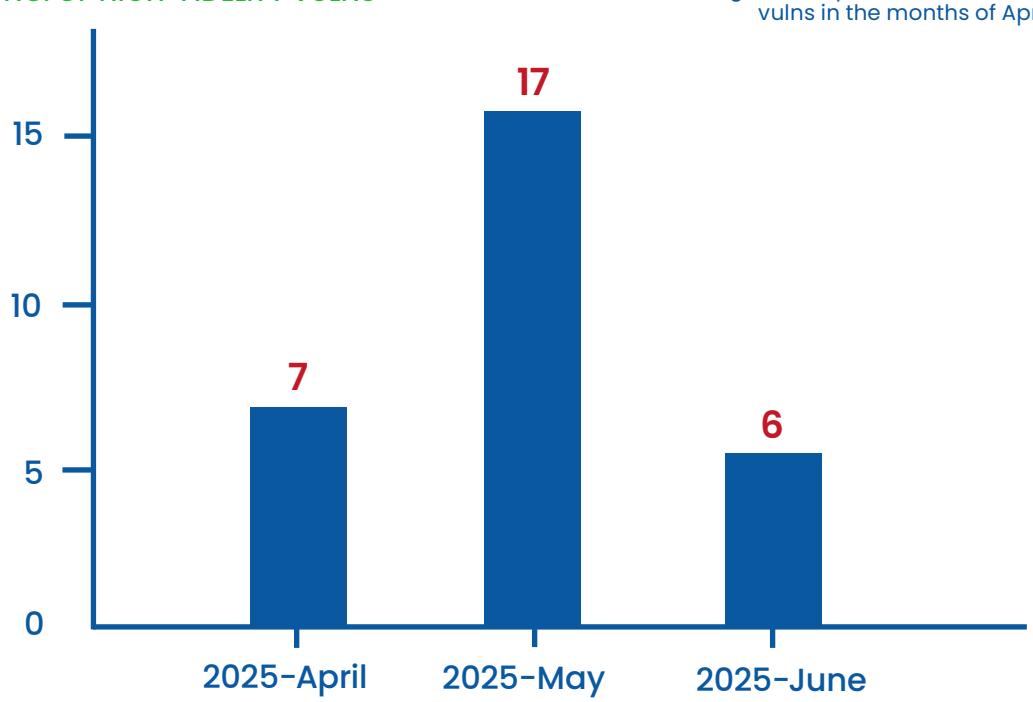
MONTHLY NO. OF WIDELY EXPLOITED VULNS

Figure 6: Depicts the total no. of widely exploited vulns in the months of April, May & June



MONTHLY NO. OF HIGH-FIDELITY VULNS

Figure 7: Depicts the total no. of high-fidelity vulns in the months of April, May & June



Along with detecting vulnerabilities, knowing which ones are already being weaponized in the wild is what makes Unified Security Intelligence (USI) indispensable. By continuously ingesting global exploit data and cross-referencing it against your asset inventory, USI brings the most urgent vulnerabilities into sharp focus:

- In April, 16 vulnerabilities showed active exploitation.
- In May, that spiked to 22, underscoring adversaries' rapid pivoting to new attack avenues.

Even as total CVE volume eased in June, 9 widely exploited vulnerabilities remained, highlighting persistent high-risk exposures.

RISK INSIGHT

Without intelligence-driven mapping to critical assets, widely exploited and high-fidelity vulnerabilities can silently compromise your most vital systems before traditional scan cycles can catch up. The only way to mitigate these risks is to continuously scan your IT infrastructure and avoid periodic scans.

Top 10 Affected Vendors/ Products

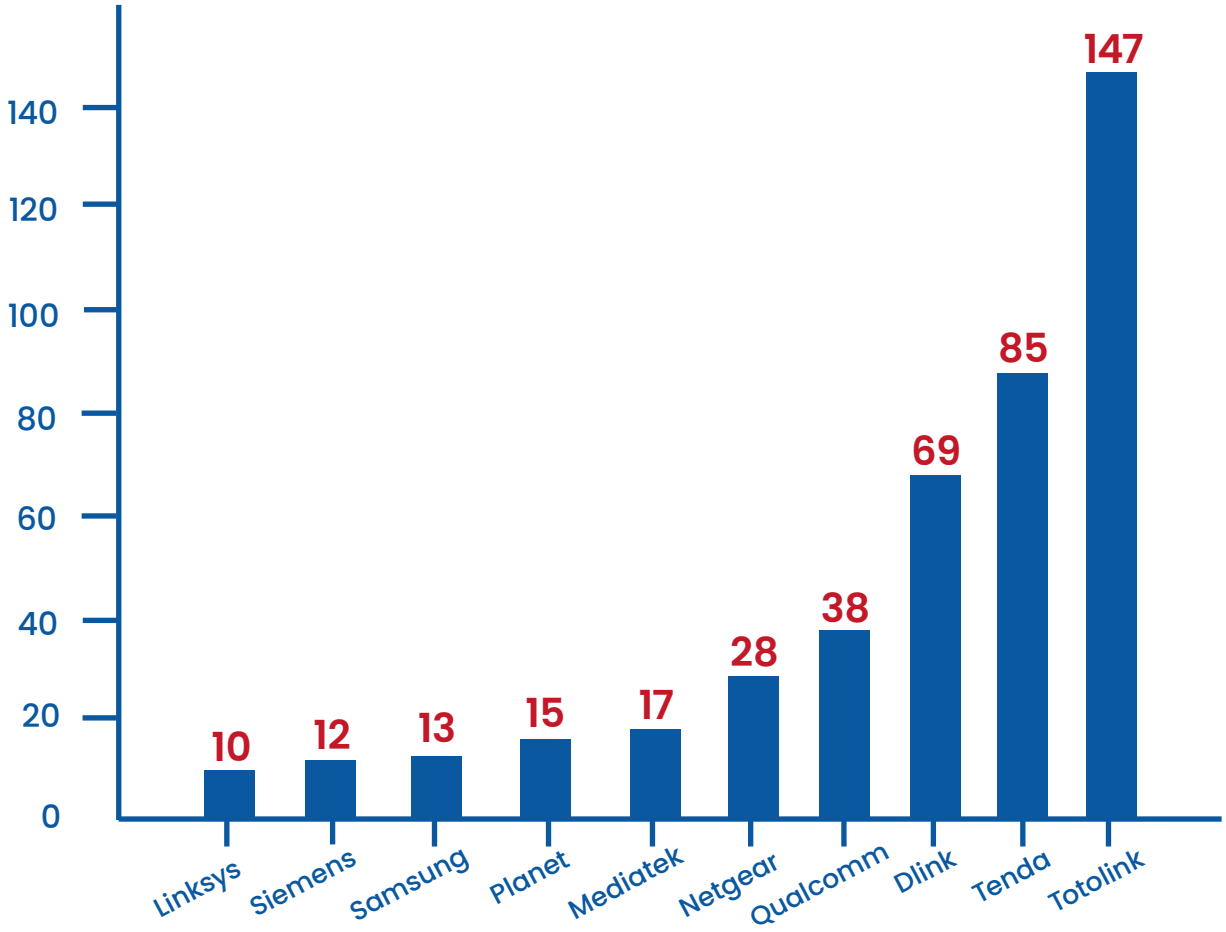


Figure 8: Shows the top affected vendors

USI can contextualize exposure across the IT landscape. One of them is understanding which hardware vendors are repeatedly and disproportionately exposed to risk.

The chart here reveals a clear risk concentration among specific hardware vendors, with Totolink, Tenda, and D-Link emerging as the most affected. Together, these three alone accounts for nearly 70% of the vulnerabilities in the top 10 list.

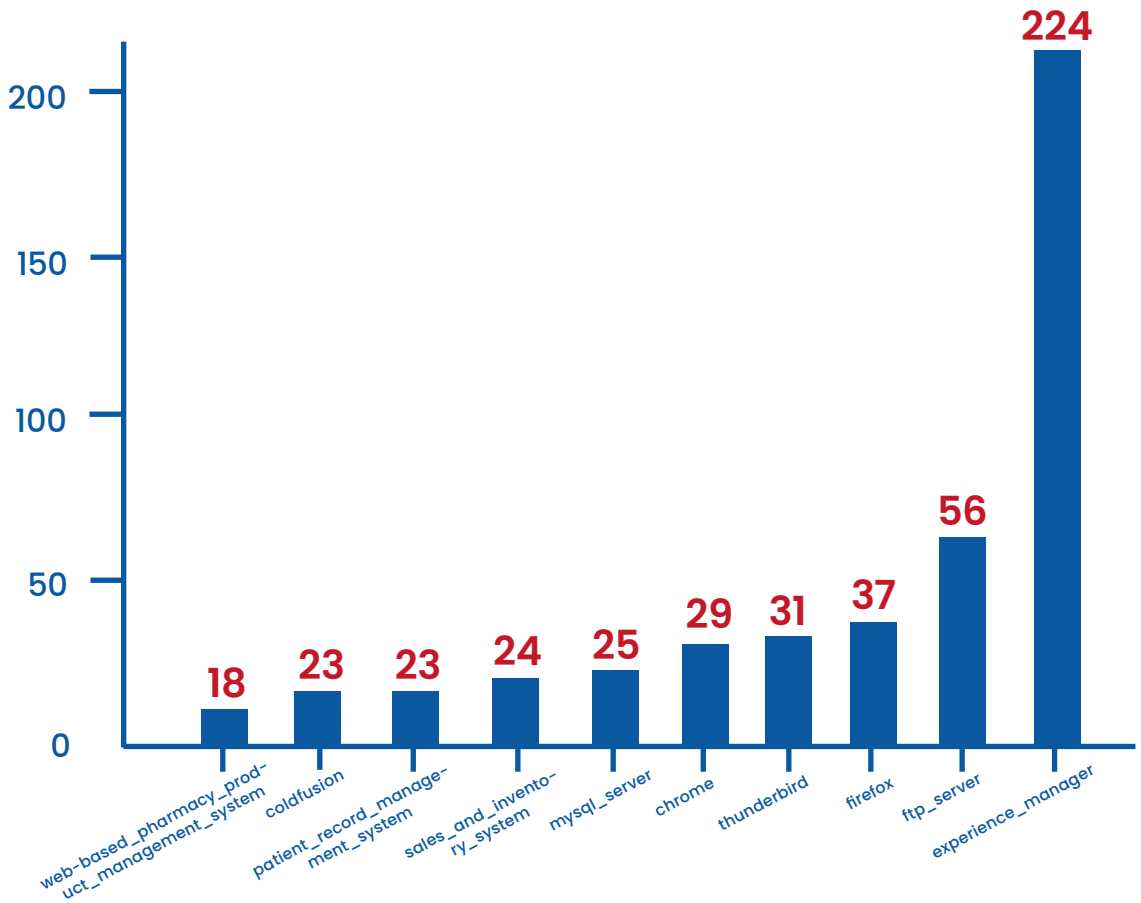


Figure 9: Shows the top affected Apps

USI not only covers hardware, but also application stack. Applications are increasingly the frontline of exploitation, often targeted due to weak access controls, unpatched CVEs, and exposed services.

This chart highlights the Top 10 Most Affected Applications, and the disparity is striking. While several apps show moderate vulnerability counts in the 20-50 range, Adobe Experience Manager surges ahead with 224 known vulnerabilities, over 4x more than the next application on the list.

1. Adobe Experience Manager dominates the threat landscape, pointing to:
    - Widespread use in web CMS deployments
    - Complex plugin ecosystems with high exposure
    - History of persistent RCE, XSS, and privilege escalation vulnerabilities
2. Applications like FTP servers, Firefox, and Thunderbird also appear prominently, reinforcing that even core IT tools carry substantial risk.

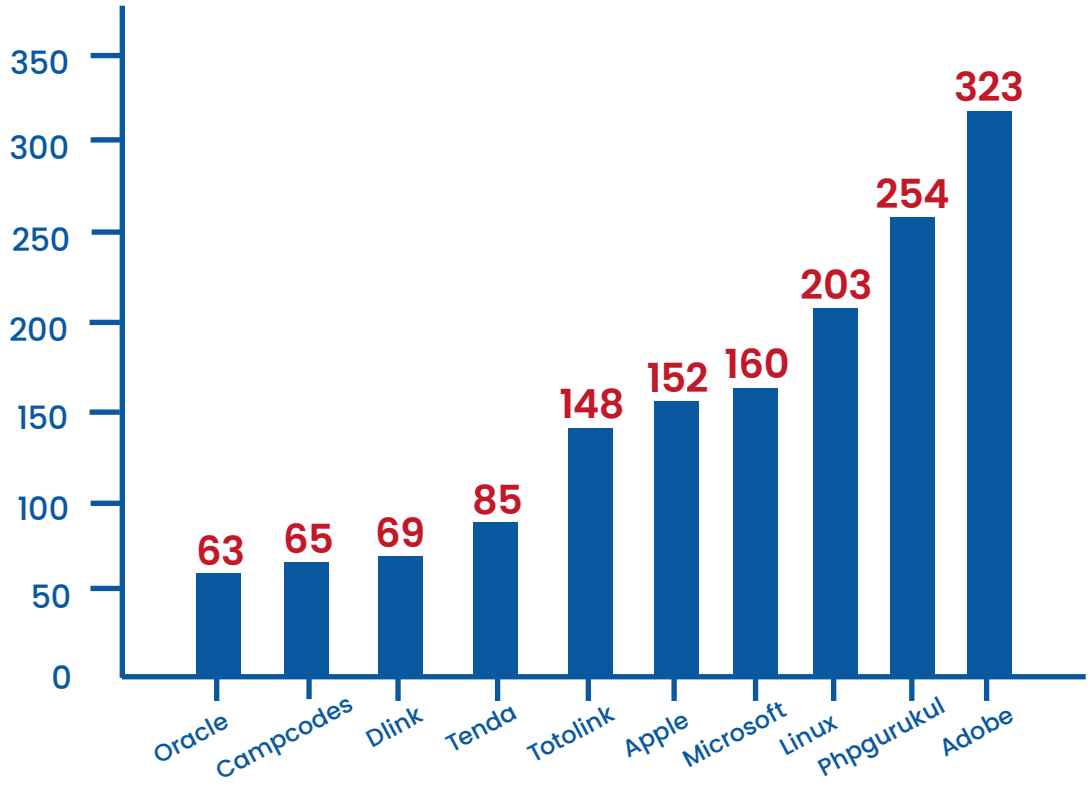


Figure 10: Shows the top affected vendors

Unified Security Intelligence (USI) doesn't just tally CVEs, it correlates them with exploit data and your own asset criticality to reveal which vendor ecosystems pose the greatest risk.

In Q2, Adobe led the pack with 323 vulnerabilities, followed by PHPgurukul (254), Linux (203), Microsoft (160) and Apple (152). This vendor-centric view empowers security teams to:

1. Allocate remediation resources toward the most exposed platforms.
2. Track patch adoption by vendor to ensure high-risk ecosystems aren't left behind.
3. Prioritize threat hunting efforts where exploit activity is both frequent and impactful.

By focusing on these top-ten vendors, USI helps shrink your attack surface where it matters most.

RISK INSIGHT

It is clearly seen that risk is highly concentrated, not uniformly spread. A small number of platforms, devices, and applications account for the majority of critical vulnerabilities, making them prime targets for attackers. This clustering of risk means:

- Remediation efforts must be prioritized toward areas with persistent exposure.
- Patch adoption and exploit trends should guide proactive defense.
- Even essential infrastructure and widely used tools can become silent weak links if left unmonitored.

By pinpointing where vulnerabilities, exploitability, and exposure converge, USI enables faster, smarter risk reduction across your environment.

Know more about patch management.

Top 10 affected Operating Systems

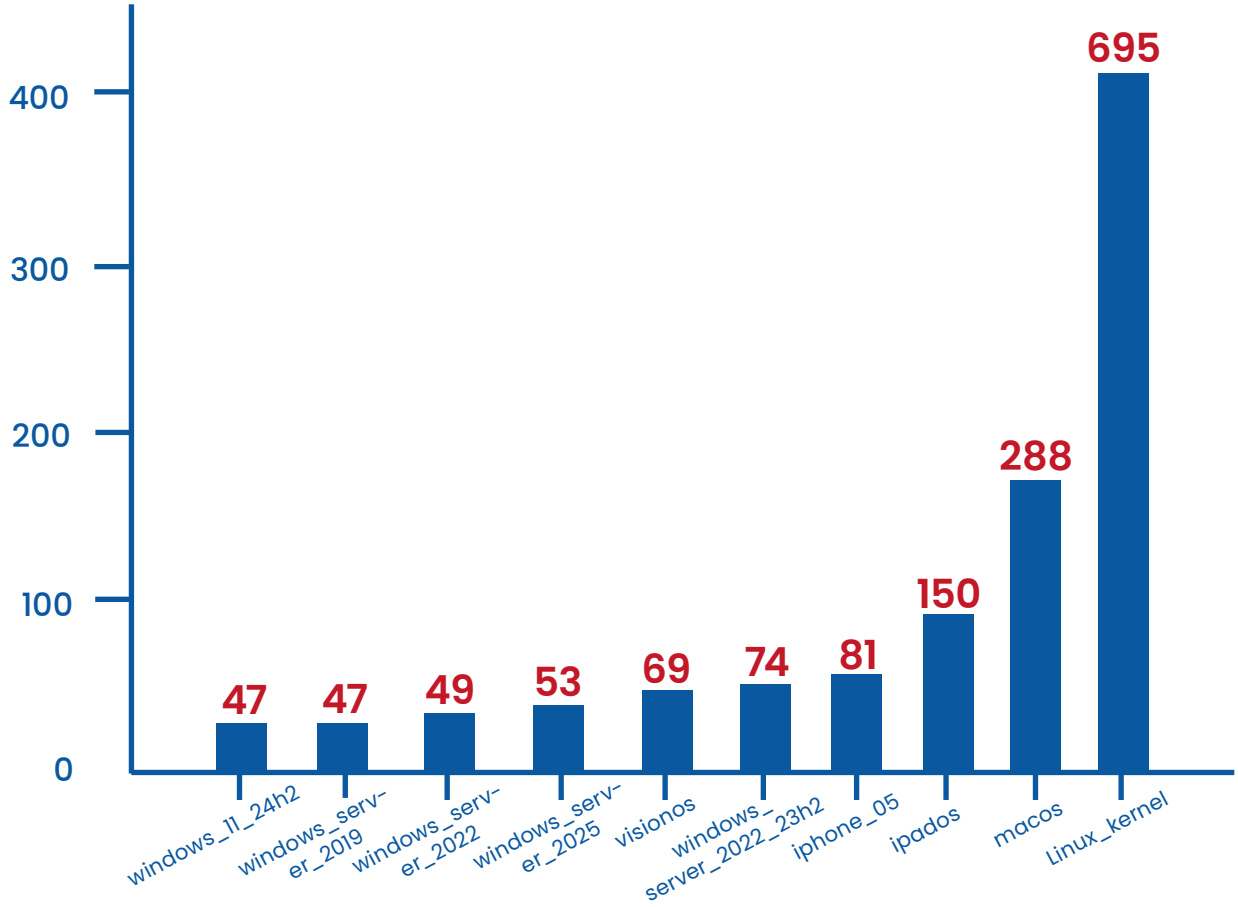


Figure 11: Shows the top affected operating systems

USI considers operating systems form the foundation of enterprise risk. Linux Kernel leads significantly, with nearly 3 times the vulnerabilities of macOS, followed by iPadOS, iPhoneOS, windows server, windows 11, and VisionOS. This highlights the critical need for kernel-level visibility and faster patch adoption in environments heavily dependent on Linux. macOS and mobile operating systems (iPadOS and iPhone OS) also show high exposure, reflecting the growing complexity and attack surface in consumer-to-enterprise hybrid devices.

RISK INSIGHT

There is a sharp concentration of vulnerabilities at the kernel and OS level. The high volume of issues in certain platforms highlights the need for deep visibility and faster patching.

Top 10 Critical Vulnerability List

Sl. No.	CVE-ID	CVSS Score	Product	Description	Impact
1	CVE-2025-53770	9.8	Microsoft SharePoint Server	Unauthenticated deserialization RCE vulnerability allowing remote code execution & credential theft.	Full server compromise, persistent backdoors, token forgery.
2	CVE-2025-22457	9.8	Ivanti Connect Secure / Policy Secure / ZTA	Stack-based buffer overflow via headers enabling unauthenticated RCE.	System takeover, malware deployment, credential compromise.
3	CVE-2025-22224	9.3	VMware ESXi / Workstation / Fusion	TOCTOU race in VMCI enabling heap-based overflow via guest VM.	VM escape, full host system compromise.
4	CVE-2025-32432	10	Craft CMS	Unauthenticated PHP object injection via insecure deserialization.	Remote server takeover on exposed web instances.
5	CVE-2025-32818	7.5	SonicWall Gen7/ Gen8 SSLVPN	Null-pointer dereference causing firewall crash (DoS).	Loss of connectivity, security appliance unresponsive.
6	CVE-2025-22225	8.2	VMware ESXi	Arbitrary kernel write via VMX process.	Full sandbox escape and host-level privilege escalation.
7	CVE-2025-22226	7.1	VMware Workstation / Fusion / ESXi	HGFS OOB read disclosing sensitive host memory.	Information disclosure, potential data leaks.
8	CVE-2025-31324	10	SAP NetWeaver (Visual Composer)	Missing authentication on file uploader allowing RCE.	Full application compromise via malicious file upload.
9	CVE-2025-32756	9.6	FortiVoice / FortiMail / FortiNDR	HTTP hash cookie triggers stack overflow enabling RCE.	Remote root access and system takeover.
10	CVE-2025-23016	9.3	FastCGI fcgi2 (IoT / Embedded)	Heap buffer overflow via crafted FastCGI requests.	Unauthenticated RCE on embedded/IoT systems.

RISK INSIGHT

Viewing these vulnerabilities from a USI standpoint, shows that recent vulnerabilities aren't just numerous, they're highly weaponizable. The top CVEs include unauthenticated remote code execution, kernel-level privilege escalation, & VM escape. These cause severe business impact ranging from full system compromise significantly increasing the risk of lateral movement, privilege escalation, and long-term persistence within large IT environments.

Zero Day Vulnerability List

Sl. No.	CVE-ID	CVSS Score	Severity	Product	Description
1	CVE-2025-1976	6.7	Medium	Brocade Fabric OS	Local admin injection flaw in IP validation enabling root-level arbitrary command/code execution
2	CVE-2025-22457	9.8	Critical	Ivanti Connect Secure / Policy Secure / ZTA Gateway	Stack-based buffer overflow in Ivanti Connect Secure VPN - unauthenticated remote code execution
3	CVE-2025-29824	7	High	Microsoft Windows CLFS driver	Use-after-free in Windows CLFS driver allowing local SYSTEM escalation
4	CVE-2025-30397	7.5	High	Microsoft Edge (IE mode)	Type confusion in Microsoft Scripting Engine (Edge IE mode) - remote RCE
5	CVE-2025-30400	7.8	High	Microsoft Windows DWM	Use-after-free in Windows DWM Core Library - local privilege escalation
6	CVE-2025-31200	7.5	High	Apple Core Audio (iOS/macOS/tvOS)	Memory corruption in Apple Core Audio via malicious audio - remote code execution
7	CVE-2025-31201	6.8	Medium	Apple OS	Pointer Authentication bypass in Apple–requires arbitrary read/write access
8	CVE-2025-31324	10	Critical	SAP NetWeaver	Unauthenticated file upload in SAP NetWeaver - full system takeover
9	CVE-2025-32701	7.8	High	Microsoft Windows CLFS driver	Use-after-free in Windows CLFS driver - local SYSTEM privilege escalation
10	CVE-2025-32706	7.8	High	Microsoft Windows CLFS driver	Input validation flaw in Windows CLFS driver - local SYSTEM escalation
11	CVE-2025-32709	7.8	High	Microsoft Windows afd.sys	Use-after-free in Windows WinSock afd.sys - local SYSTEM escalation
12	CVE-2025-32756	9.6	Critical	FortiMail, FortiVoice, FortiNDR, FortiRecorder, FortiCamera	Stack-based buffer overflow in Fortinet devices admin API - unauthenticated remote code execution
13	CVE-2025-33053	8.8	High	Microsoft WebDAV / Internet Shortcuts	External control of filename/path in WebDAV/shortcut - remote code execution
14	CVE-2025-4427	5.3	Medium	Ivanti Endpoint Manager Mobile (EPMM)	Authentication bypass in Ivanti EPMM Mobile API - unauthenticated access to protected resources

Sl. No.	CVE-ID	CVSS Score	Severity	Product	Description
15	CVE-2025-4428	8.8	High	Ivanti Endpoint Manager Mobile (EPMM)	Post-authenticated API RCE in Ivanti EPMM via crafted requests
16	CVE-2025-6543	9.2	Critical	Citrix NetScaler ADC / Gateway	Memory overflow in Citrix NetScaler ADC/Gateway control-flow hijack or DoS

RISK INSIGHT

Analysis of these CVEs reveals remote-code-execution (RCE) in critical network and application gateways (e.g., stack-based buffer overflows and file-upload flaws), and local privilege-escalation vectors in core OS and driver components (use-after-free, pointer-authentication bypass). By mapping these vulnerabilities against exploits, asset inventories, and networks, USI can enable security teams to prioritize patching efforts.

Misconfigurations

CCE-ID	Description	CCSS
CCE-66368-2	This setting controls whether domain controllers permit Netlogon secure channels without Secure RPC for specified machine accounts. Apply it via GPO on the Domain Controllers OU across the forest.	10
CCE-66374-0	This setting controls whether WebAuthn requests in a Remote Desktop session are redirected to the user's local authenticator (e.g., Windows Hello for Business or a security key).	10
CCE-95475-0	nftables is the Linux kernel's packet-filtering framework (iptables' successor) installed with firewalld. To avoid clashes, mask & stop it when firewalld is in use.	10
CCE-70969-1	Ensure SELinux is set to enforcing or permissive mode to maintain security policy enforcement. Disabling SELinux is discouraged as it halts enforcement and removes object labeling, hindering future reactivation.	10
CCE-76068-6	Ensure the pam_unix.so module does not use the nullok option, which allows blank passwords. Disabling nullok enforces strong authentication and prevents unauthorized access.	9.9
CCE-76072-8	Ensure the root account has a password set or is locked to prevent unauthorized system control. Unsecured root access poses a critical security risk.	9.9
CCE-76096-7	Ensure only the root account has a primary GID of 0 to maintain strict privilege separation. Sharing GID 0 with other users can lead to unauthorized access to root-owned resources.	9.9
CCE-99442-6	Disable or remove the DNS server (bind9) on systems not intended to provide DNS services. This minimizes the system's attack surface and improves overall security	9.9
CCE-66213-0	Enable this setting to allow devices to authenticate to the domain using certificates via Kerberos. It enhances security by supporting certificate-based authentication, falling back to passwords if set to Automatic.	9.8
CCE-66270-0	Set a minimum password length of 14 characters to enhance security and resist brute-force attacks. Longer passphrases are more secure and user-friendly than complex short passwords.	9.8

RISK INSIGHT

These misconfigurations weaken system hardening, access control, and authentication, increasing exposure to privilege escalation, unauthorized access, and service misuse. Disabling key protections like SELinux, allowing insecure Netlogon or blank passwords, and running unnecessary or conflicting services significantly broadens the attack surface. USI can quickly detect these flaws and provide the right fixes to remediate them.

Top 10 Malware Vulnerability Enumeration

MVE ID	Threat Name	Type
MVE-000846	Trailblaze	Malware
MVE-000847	RESURGE	Malware
MVE-000848	PipeMagic	Trojan
MVE-000850	DslogdRAT	Malware
MVE-000821	SideWalk	Backdoor
MVE-000836	MATA	Backdoor
MVE-000831	RansomHub	Ransomware
MVE-000833	Murdoc	Botnet
MVE-000859	Qilin	Ransomware
MVE-000860	Resbot	Botnet

RISK INSIGHT

Malwares can enable stealthy access and large-scale compromise. It includes ransomware extort operations by leveraging advanced evasion. A layered defense powered by USI can drive continuous monitoring, strict security controls, and rapid risk remediation.

Top 10 Posture Anomalies

Anomaly Name	Anomaly ID	Category	Description
Vulnerable process making outbound network connection	PA-2022-1001	Risk	Identifies vulnerable processes making external network connections—flagged as anomalous port-specific behavior.
Unusual tasks are scheduled in Task Scheduler	PA-2022-1011	System	Detects unusual scheduled tasks in Windows Task Scheduler, indicating possible malicious or unauthorized automation.
Firewall disabled	PA-2022-1033	System Security	Detects systems where the firewall is disabled, exposing devices to unfiltered network traffic.
UAC policy not configured properly	PA-2022-1034	System Security	Flags systems where User Account Control (UAC) is misconfigured, reducing resistance to unauthorized privilege escalation.
ASLR is disabled	PA-2022-1036	System Security	Identifies devices where Address Space Layout Randomization (ASLR) is turned off, increasing the risk of memory-based attacks.
Anomaly found in users with elevated privilege	PA-2022-1021	System Security	Detects unexpected or anomalous elevated/sudo user privileges that can lead to unauthorized access or data compromise.
Irregular Host IP to MAC address maps	PA-2022-1003	Network	Flags anomalies in ARP tables where Host IP-to-MAC mappings are inconsistent—may indicate spoofing or misconfigurations.
Increasing Critical Vulnerability Count	PA-2022-1017	Risk	Monitors and alerts on devices showing a rising trend in critical vulnerabilities, using anomaly detection techniques.
Unique software applications on few systems	PA-2022-1002	Software Assets	Identifies rare software installed only on a few systems within a cluster, indicating potential shadow IT or risk.
Anomalous events in Windows Event log	PA-2022-1004	Events	Detects blacklisted or suspicious events (e.g., failed logins, multiple login attempts, account updates) using event log analysis.

RISK INSIGHT

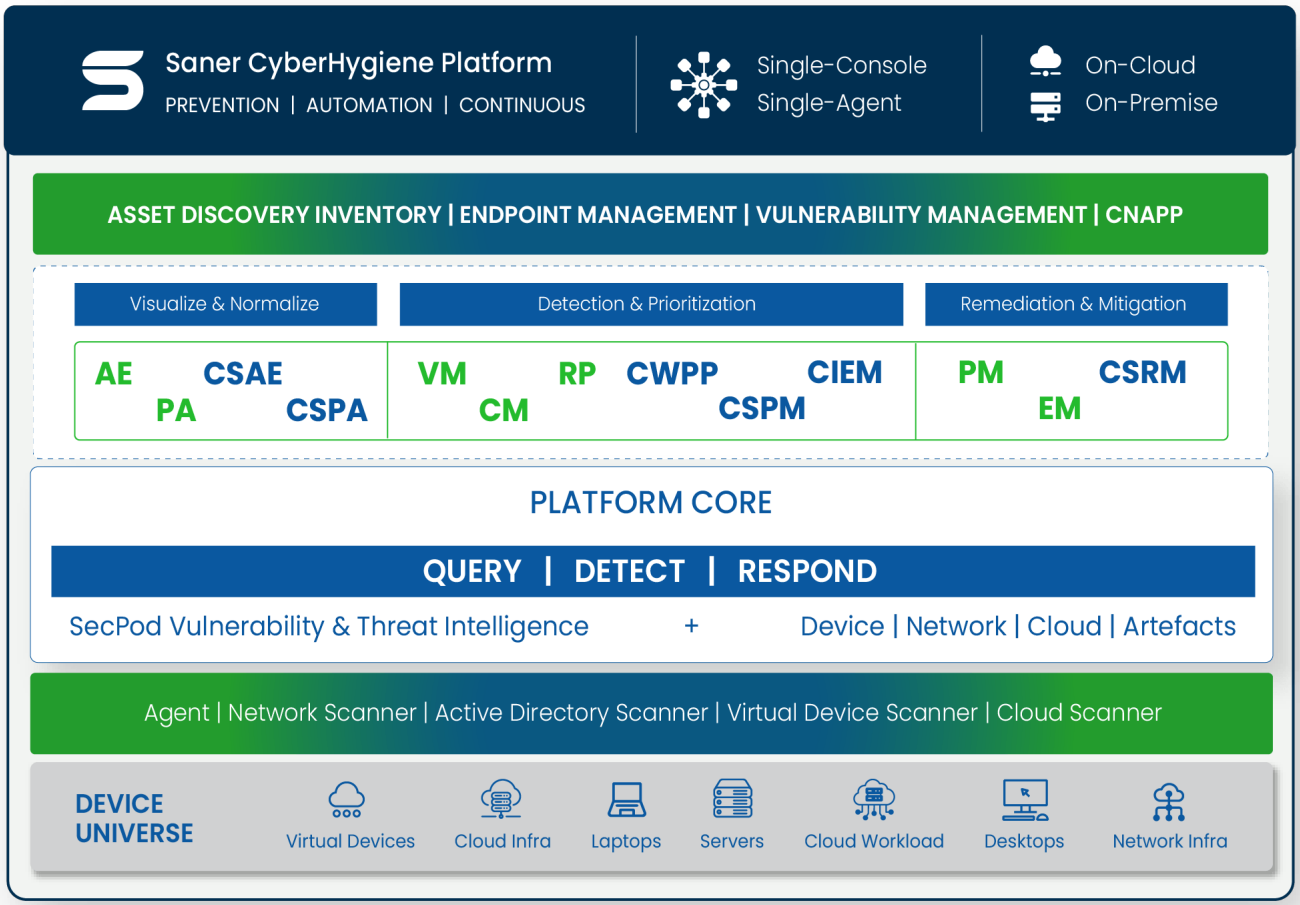
These posture anomalies reveal deep-rooted weaknesses across system configurations, user privileges, software assets, and network behavior which can get exploited.
USI enables continuous visibility and contextual correlation of such anomalies, transforming isolated signals into actionable risk intelligence. By normalizing and prioritizing these anomalies, USI shifts organizations to more proactive risk remediation.
Know more about posture anomaly management.

Scan, Normalize, Detect, Prioritize & Remediate Endpoint & Cloud Security Risks with Saner

Saner Platform is a suite of solutions that help organizations establish a strong security posture to proactively prevent attacks in endpoints and the cloud.

SANER CLOUD – An AI-fortified Cloud-Native Application Protection Platform (CNAPP) that delivers continuous visibility, security compliance, and risk mitigation for cloud environments.

SANER CVEM – A Continuous Vulnerability and Exposure Management (CVEM) solution that delivers continuous visibility, identifies, assesses, and remediates vulnerabilities across enterprise devices and network infrastructure.



SecPod is a leading cybersecurity technology company committed to preventing cyberattacks through proactive security. Its mission is to secure computing infrastructure by enabling preventive security posture.

At the core of SecPod's offerings is the Saner Platform - a suite of solutions that help organizations establish a strong security posture to preempt cyber threats against endpoints, servers, network and cloud infrastructure, as well as cloud workloads. With its cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

info@secpod.com

secpod