Q1 Vulnerability Report

www.secpod.com

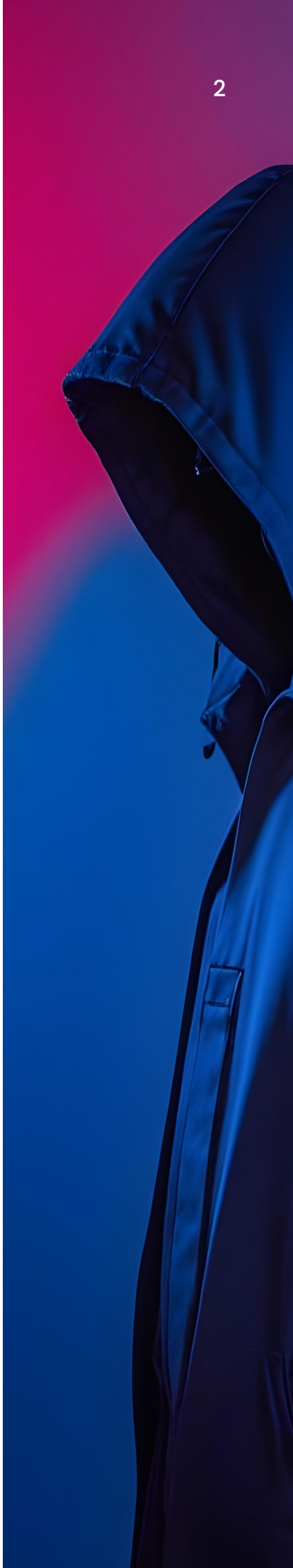
2025 Vulnerability Report

As we step into 2025, the cybersecurity landscape is already marked by rapid change, increasing complexity, and a relentless rise in threats. The first quarter alone has witnessed **12011 vulnerabilities, reflecting a 7.93% increase** from the previous period, with 13 zero-day vulnerabilities already uncovered. These figures underscore the growing urgency for proactive and intelligent security strategies.

To help organizations navigate this dynamic environment, we are proud to present a comprehensive, detailed quarterly report. This report offers a powerful look into the vulnerabilities, threats, and trends shaping the security posture of modern enterprises across all layers of the digital stack.

KEY HIGHLIGHTS:

- More than **12000 risks** detected in the first three months of 2025
- **13 zero-day vulnerabilities** were uncovered
- **Linux Kernel** is the top-affected operating system with over 690 vulnerabilities
- A total of **5307 vulnerabilities** were under high and critical vulnerabilities
- By the end of 2025, SecPod predicts **40000 vulnerabilities**



With projections suggesting more than 40,000 vulnerabilities by year's end, the need for robust and advanced cybersecurity solutions is clear. This report examines the risks, where they are most densely concentrated, how quickly they should be addressed, and why prioritization is more critical than ever.

At its core, the quarterly report is a call to action: to stay informed, to act decisively, and to protect proactively. Whether you're a CISO shaping security strategy or a practitioner on the front lines, this report is crafted to empower your decisions in 2025 and beyond.

Join us in decoding the current vulnerability and exposure landscape and building a more resilient security posture.

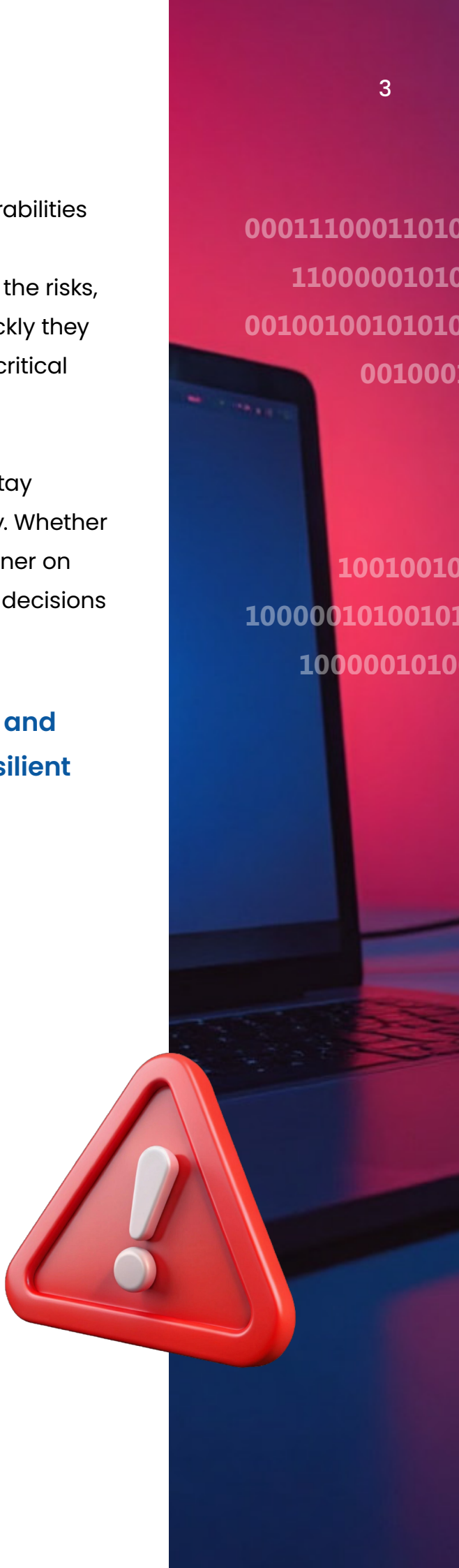


Table of Contents

Report Coverage

This section outlines the scope and depth of the security assessment conducted. It summarizes key metrics such as the total number of identified vulnerabilities, including zero-day and high/critical issues, misconfigurations, patches covered, and Linux-specific vulnerabilities.

These insights provide a foundational understanding of the current security landscape and highlight areas requiring immediate attention.

12011

Total No. of Vulnerabilities

13

Zero-Day Vulnerabilities

5307

High & Critical Vulnerabilities

1491

Total No. of Misconfigura-tions

1484

Total No. of Patches Covered

694

Linux Vulnerabilities

Detailed Insights into Risks

In any modern digital environment, risk is an unavoidable part of operations, but not all risks are the same.

Security Risks – These involve risks that can lead to data breaches, unauthorized access, or malicious attacks.

Here are a few risks that fall into the above categories:

VULNERABILITIES

Weaknesses in software or systems that can be exploited by attackers. These may arise from outdated software, code flaws, or unpatched systems.

MISCONFIGURATIONS

Incorrect or insecure settings that unnecessarily expose systems. This is one of the most common root causes of breaches.

POSTURE ANOMALIES

Deviations from your organization's defined security baseline, such as unwanted processes or ports.

EXPOSURES

Assets, data, or services that are unintentionally left accessible (e.g., public-facing S3 buckets or open ports) can be discovered by attackers.

In this report, let's dig deep into each one of them.

Total Number of CVEs Covered

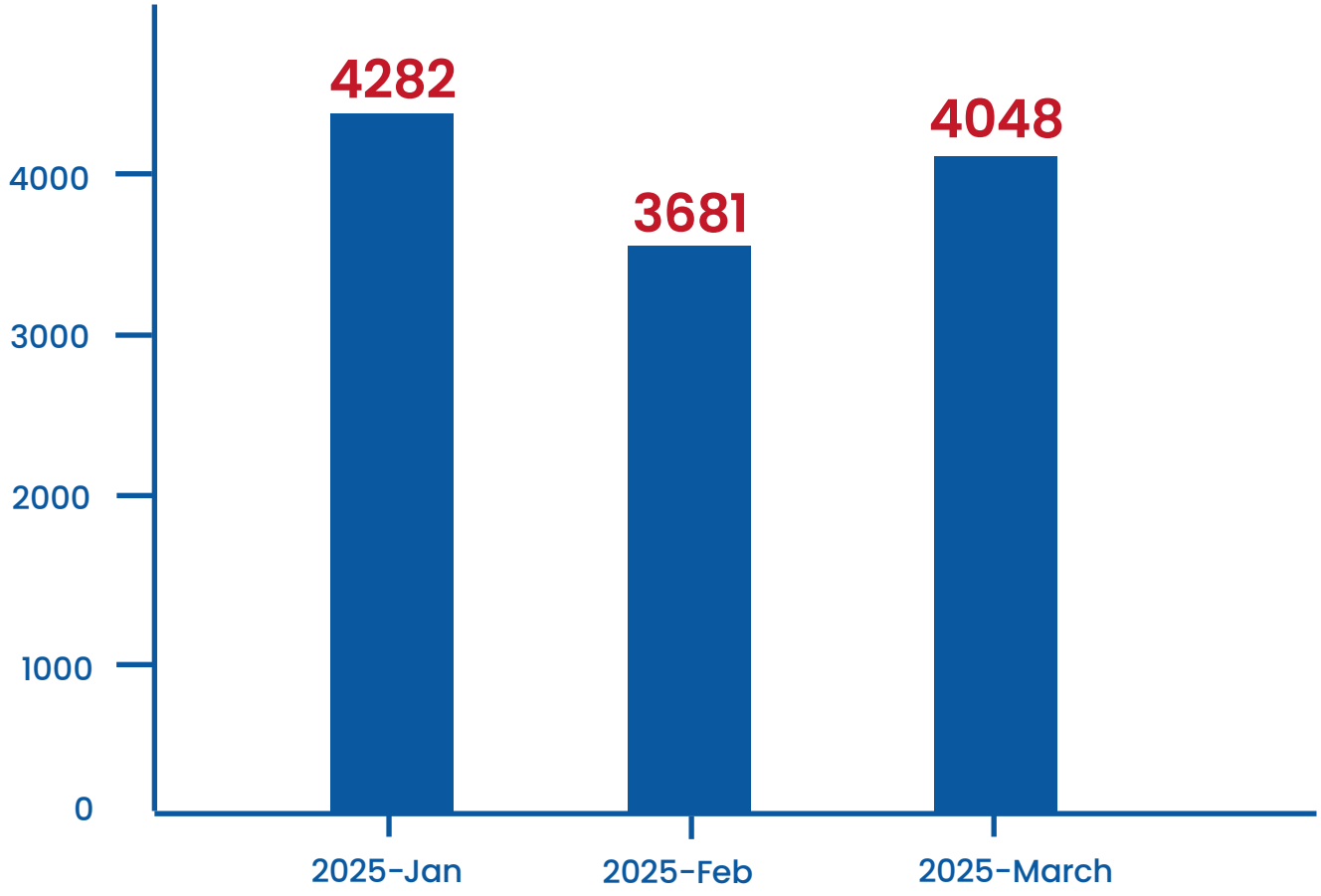


Figure 1: Shows the Number of vulnerabilities published from January to March 2025

The chart illustrates the monthly number of vulnerabilities identified in the first quarter of 2025. January recorded the **highest count with 4,282 vulnerabilities,** indicating a period of heightened exposure—potentially due to year-end backlog or newly disclosed threats. In February, the number dropped to 3,681, suggesting a brief improvement or fewer disclosures during that month.

However, **March saw an uptick to 4,048,** pointing to a possible resurgence in vulnerabilities, either from emerging threats or delayed remediation. Overall, the data reflects a **consistently high volume of vulnerabilities,** underscoring the ongoing need for proactive risk management and continuous security monitoring.

Vulnerability Severity Distribution based on CVSS v3 & v4

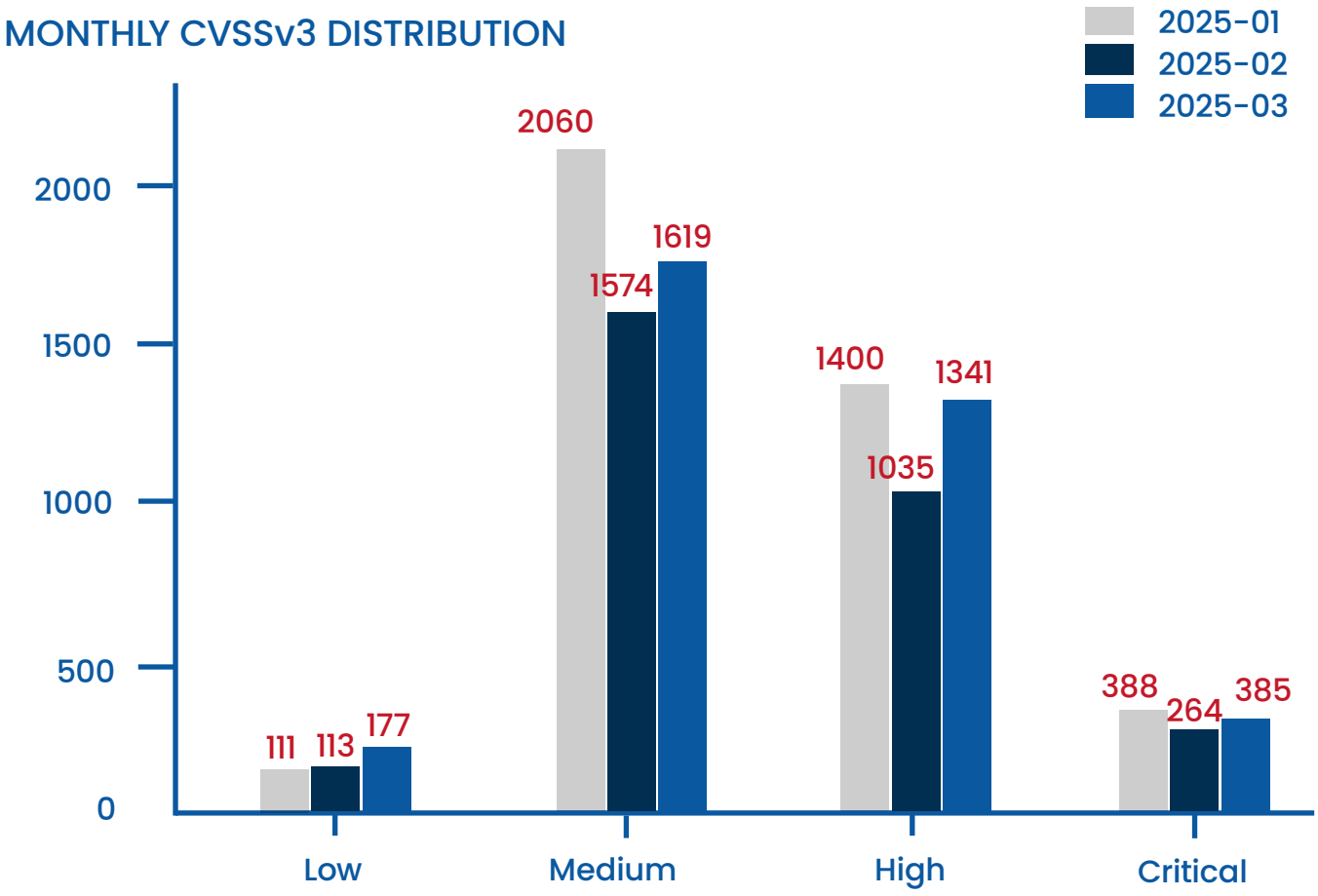


Figure 2: Depicts the vulnerability severity distribution based on CVSS v3 base score

The Common Vulnerability Scoring System (CVSS) is a standardized method to rate the severity of software vulnerabilities, helping security teams prioritize what to fix.

CVSS v3.0 focuses mainly on the technical aspects of a vulnerability, like how it can be exploited and its impact on confidentiality, integrity, and availability.

With the release of CVSS v4.0, the scoring system now includes more real-world context. It introduces new metrics such as exploitability, safety impact, and recovery difficulty, making it more relevant to modern environments.

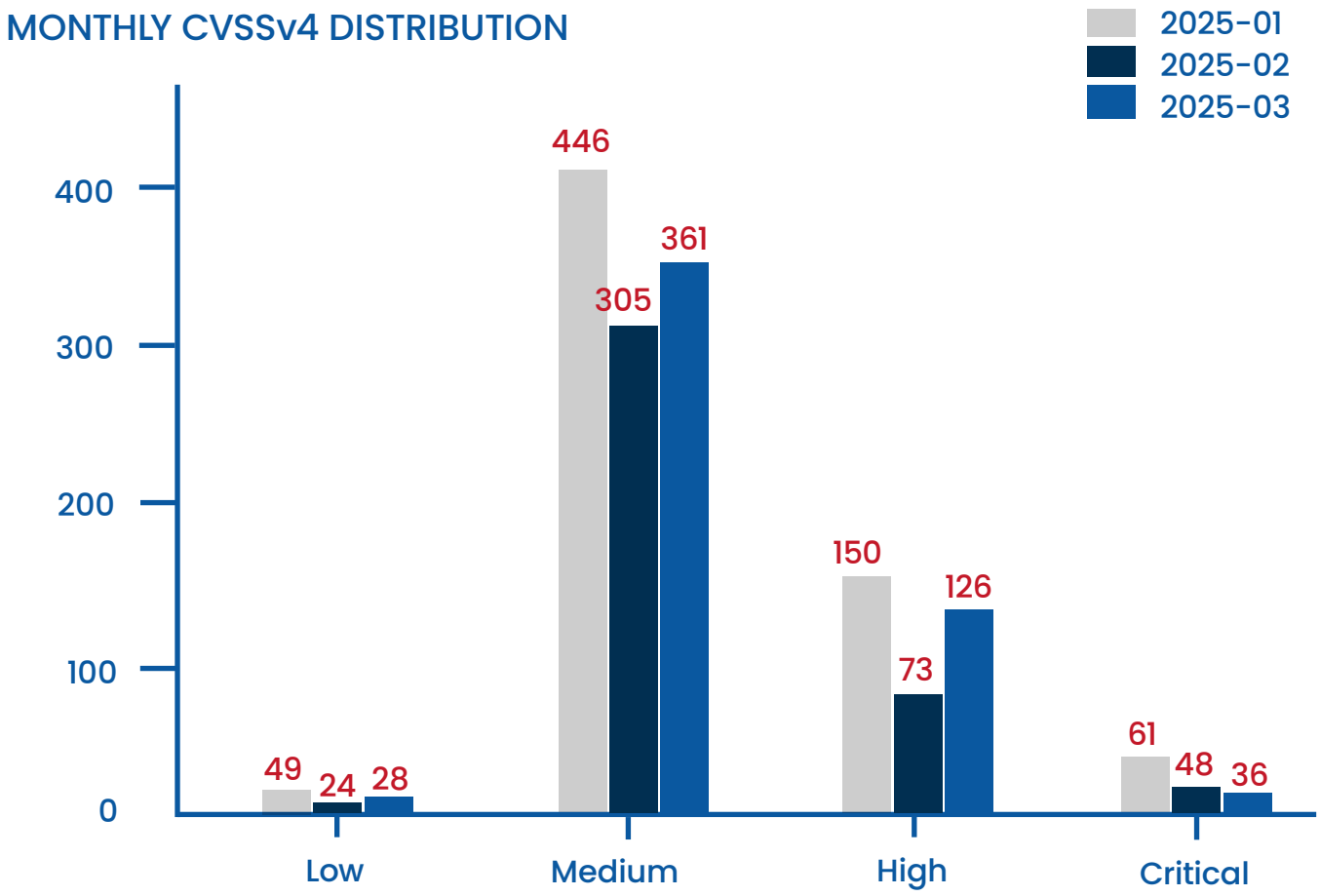


Figure 3: Depicts the vulnerability severity distribution based on CVSS v4 base score

Combining both the graphs together, here is the vulnerability categorization based on severity:

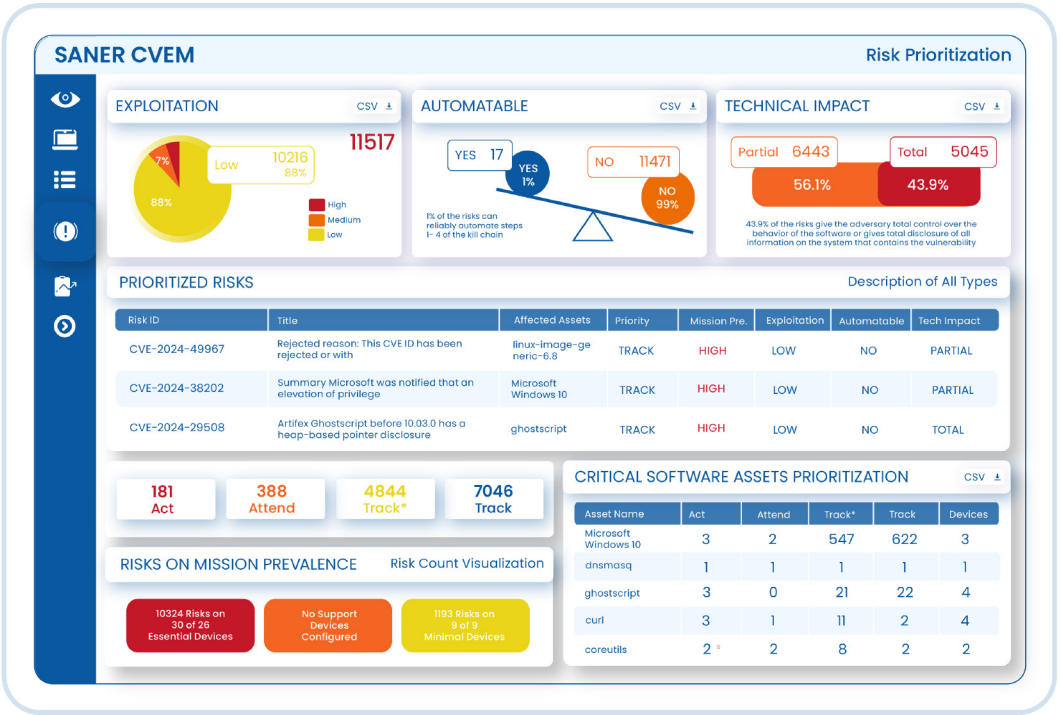
SEVERITY	JAN (2025-01)	FEBRUARY (2025-02)	MARCH (2025-03)	TOTAL
Low	160	137	205	502
Medium	2506	1879	1980	6365
High	1550	1108	1467	4125
Critical	449	312	421	1182

Over 43% of vulnerabilities are high and critical severity, highlighting the need for quick patch management solutions. However, medium-severity vulnerabilities dominate, which tells us that focusing on only high and critical risks is not enough!

This is where the concept of **CISA-SSVC-based risk prioritization** comes into the picture; no matter what severity is assigned through the CVSS score, it gets a step ahead and takes other factors such as business context, technical impact, and mission prevalence.

Experience this through Saner risk prioritization:

https://www.secpod.com/risk-prioritization/



Top 10 Affected Vendors/ Products

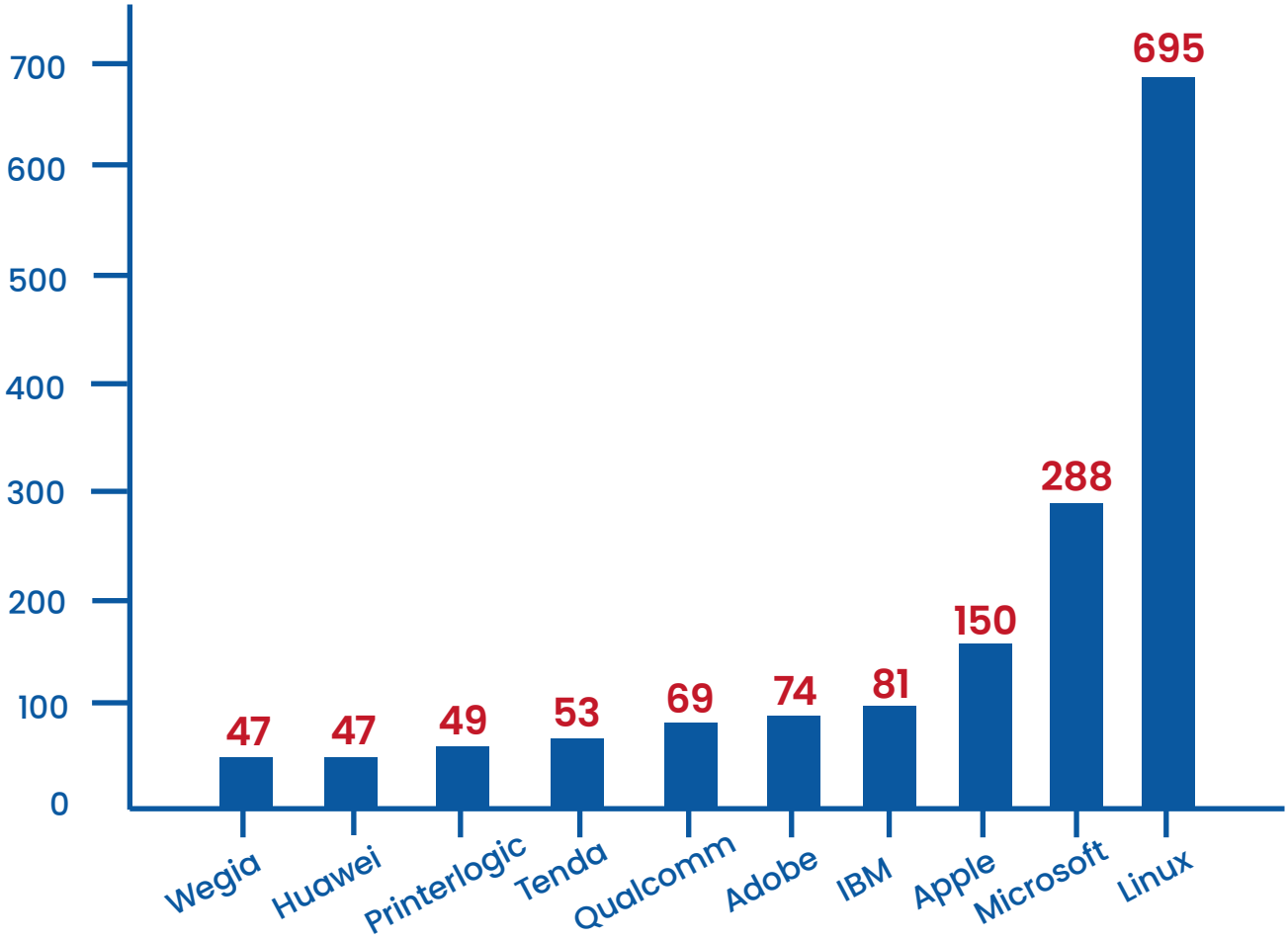


Figure 4: Shows the top affected vendors

The standout observation here is that **Linux has more than double the vulnerabilities** compared to the next highest vendor (Microsoft). This is both a reflection of its widespread use and its architectural openness.

The main reasons why Linux is always the prime target of attackers

- Linux powers more than 90% of public cloud workloads
- There are hundreds of Linux distributions, each with its own packaging, release cycles, and security models

Here are **a few common techniques hackers** might use to exploit a risk in Linux distributions:

- Privilege Escalation
- Remote Code Execution (RCE)
- Supply Chain Attacks
- Kernel Exploits

Taking all the factors into consideration, it's no surprise that the top affected operating system during the first quarter was Linux.

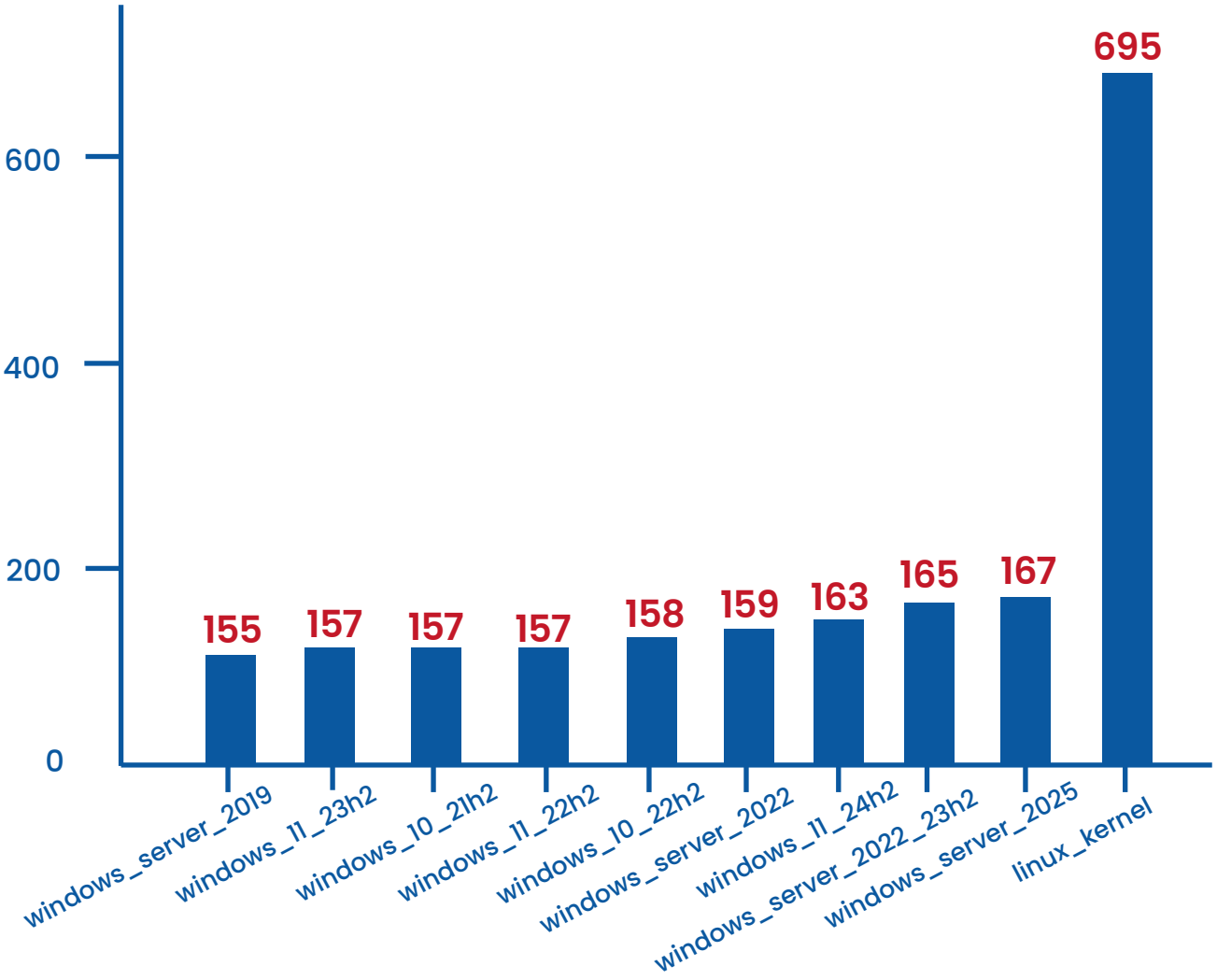


Figure 5: Shows the top affected OSs

Top 10 Affected Hardware

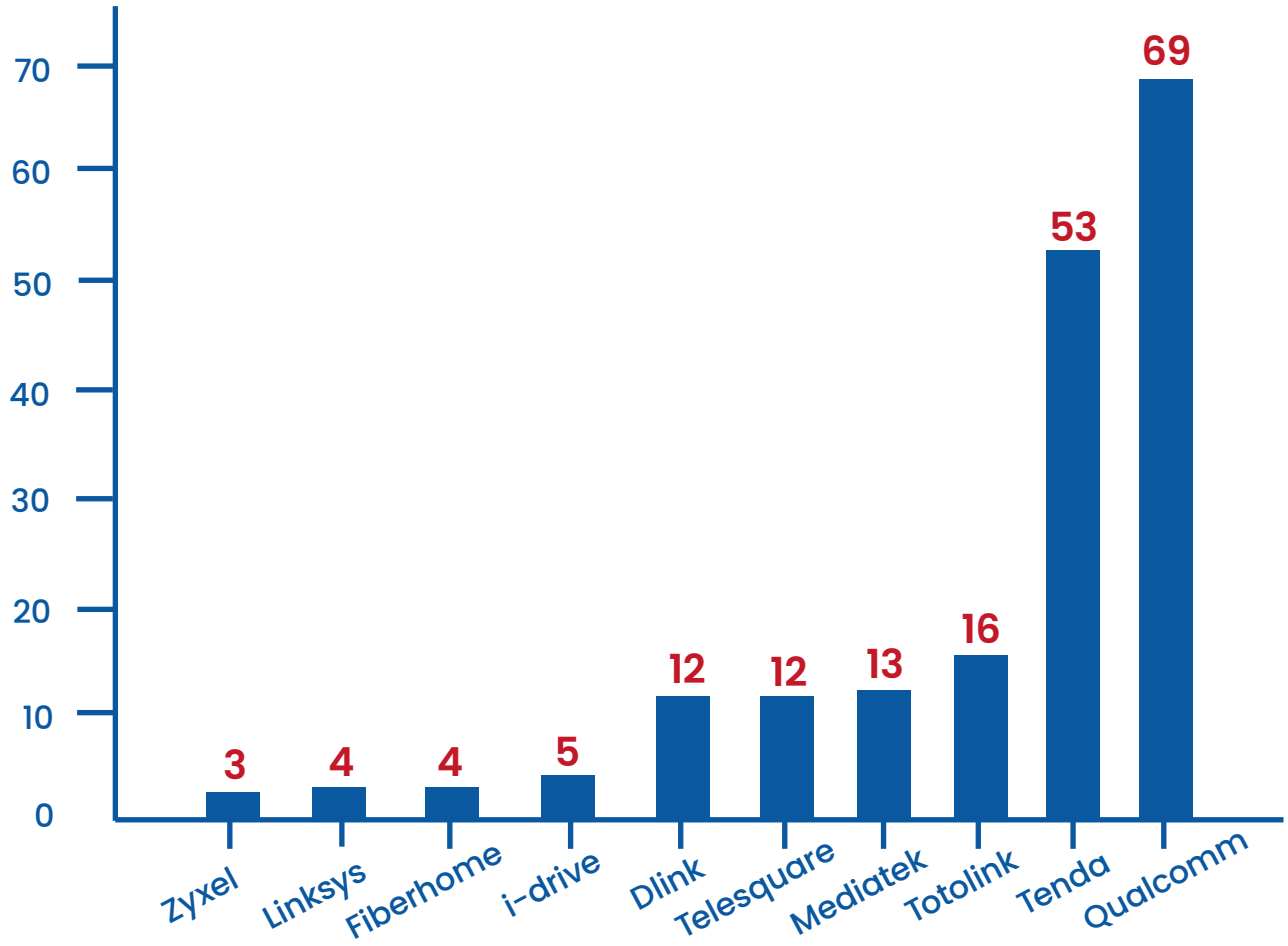


Figure 6: Shows the top affected hardwares

Qualcomm and Tenda account for over 65% of all hardware vulnerabilities reported in this data, signaling a strong focus from threat actors on embedded and networking chipsets used across the modern digital ecosystem.

Alongside, let's also take a look at the most affected applications.

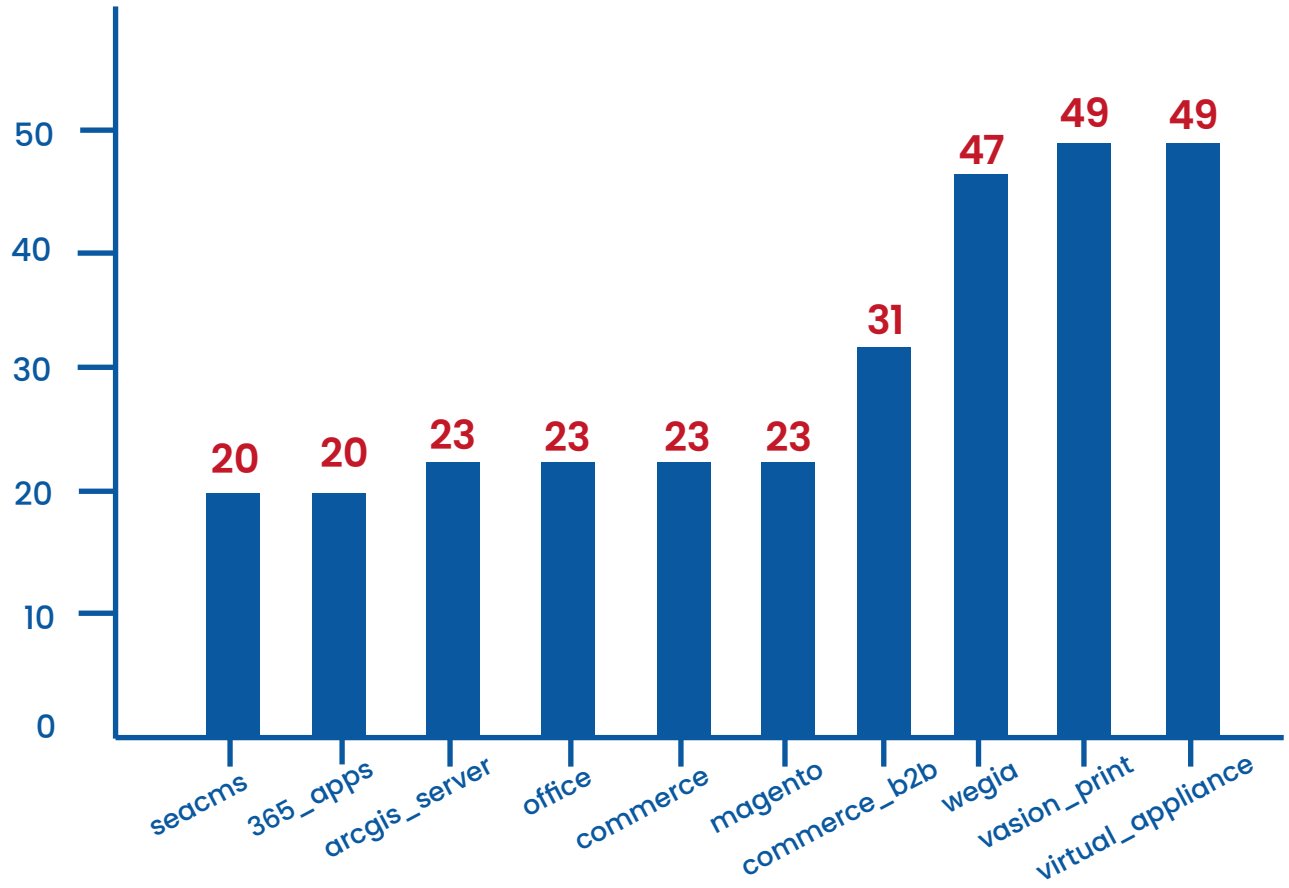


Figure 6: Shows the top most affected applications

The analysis of the "Top Affected Apps" chart reveals a concerning trend where applications like **Vasion_Print and Virtual_Appliance top the list** with the highest number of vulnerabilities (49 each). These applications often operate with elevated privileges and are deeply embedded in enterprise ecosystems, making them high-value targets for attackers.

The presence of productivity and cloud-integrated apps like Office, 365_Apps, and ArcGIS_Server underlines a broader threat landscape where attackers target both infrastructure and user-facing tools to gain access, move laterally, or exfiltrate data. The high prevalence of vulnerabilities across such varied applications highlights the urgent need for organizations to prioritize patching based on business impact and exposure rather than just CVE counts.

But what are the vulnerabilities that made a lot of noise?

Top 10 Critical Vulnerabilities

Sl. No.	CVE-ID	CVSS Score	Product	Description	Impact
1	CVE-2025-22224	9.8	VMware Products	Zero-day vulnerability actively exploited in the wild.	Remote Code Execution, Unauthorized Access
2	CVE-2025-24813	8.5	Apache Tomcat	Path equivalence vulnerability allowing remote code execution & information disclosure.	Remote Code Execution, Information Disclosure
3	CVE-2025-2783	7.9	Google Chromium	Sandbox escape vulnerability due to a logic error, affecting Chromium-based browsers.	Sandbox Escape, Elevated Privileges
4	CVE-2025-29927	8.2	Next.js	Authorization bypass vulnerability in the Next.js React framework.	Authorization Bypass, Unauthorized Access
5	CVE-2025-2825	9.0	CrushFTP	Authentication bypass vulnerability in CrushFTP file transfer server.	Authorization Bypass, Unauthorized Access
6	CVE-2025-24085	8.7	iOS 18.3.1	Critical vulnerability exploited on iOS 18.3.1.	Remote Exploitation, System Compromise
7	CVE-2025-1974	7.5	Ingress NGINX	Part of 'IngressNightmare' vulnerabilities in Ingress NGINX.	Security Risk, Unauthorized Access
8	CVE-2025-23087	8.3	Node.js	Critical security flaw in Node.js versions 17.x and earlier.	Unauthorized Access, Security Compromise

Sl. No.	CVE-ID	CVSS Score	Product	Description	Impact
9	CVE-2025-21376	8.1	Windows LDAP	Remote code execution vulnerability in Windows LDAP.	Remote Code Execution, High Risk
10	CVE-2025-21418	9.1	Windows AFD.sys (WinSock)	Privilege escalation vulnerability in Windows AFD.sys for WinSock.	Privilege Escalation, Full System Compromise

At the top of the list is CVE-2025-22224, a zero-day vulnerability in VMware products with a critical CVSS score of 9.8, actively exploited in the wild and capable of remote code execution and unauthorized access. This points to a persistent trend of attackers targeting virtualization and cloud infrastructure platforms that are central to enterprise IT environments. Likewise, CrushFTP (CVE-2025-2825) and Windows AFD.sys (CVE-2025-21418) pose major risks due to their potential for authentication bypass and privilege escalation respectively—both capable of full system compromise when exploited.

This list of critical CVEs provides a clear, prioritized view of current high-risk vulnerabilities, enabling security teams to focus patching efforts on the most severe and actively exploited flaws. By mapping these CVEs to internal systems, organizations can improve threat detection, strengthen defenses, and meet compliance requirements more effectively.

For business leaders, the list translates technical threats into actionable business insights. It supports better communication of cyber risks, informs security investment decisions, and helps organizations proactively defend against evolving threats rather than reacting after the fact.

There is also a list of zero-day vulnerabilities discovered:

Sl. No.	CVE-ID	CVSS Score	Product	Description	Impact
1	CVE-2024-55591	9.8	FortiOS, FortiProxy	Authentication bypass vulnerability allows remote attacker to gain super-admin privileges.	Authentication Bypass
2	CVE-2025-0282	9.0	Ivanti Connect Secure, Ivanti Policy Secure	Stack-based buffer overflow	Remote Code Execution
3	CVE-2025-1094	9.0	PostgreSQL	SQL injection	improper neutralization of quoting syntax
4	CVE-2025-21297	8.1	Windows Remote Desktop Services	Remote code execution	Remote code execution
5	CVE-2025-21590	6.7	Juniper Networks Junos OS	Improper isolation in the kernel	privilege escalation
6	CVE-2025-22224	9.3	VMware ESXi, Work-station	TOCTOU vulnerability	out-of-bounds write and possible code execution
7	CVE-2025-22225	8.2	VMware ESXi	Arbitrary write vulnerability	sandbox escape
8	CVE-2025-22226	6.0	VMware ESXi, Work-station, Fusion	Out-of-bounds read in HGFS	information disclosure
9	CVE-2025-23006	9.8	SonicWall SMA 1000 Series	Pre-auth deserialization vulnerability	remote command execution

Sl. No.	CVE-ID	CVSS Score	Product	Description	Impact
10	CVE-2025-23087	N/A	Node.js	High-severity vulnerability in all EOL versions of Node.js.	High-severity vulnerability in all EOL versions of Node.js.
11	CVE-2025-24085	7.8	macOS	Use-after-free vulnerability	privilege escalation
12	CVE-2025-24813	9.8	Apache Tomcat	Path traversal vulnerability	information disclosure
13	CVE-2025-2783	8.3	Google Chrome	Sandbox escape via incorrect handle in Mojo	Sandbox escape via incorrect handle in Mojo.

Zero-day vulnerabilities are security flaws that are unknown to the software vendor or developer at the time they are discovered and exploited by attackers. Because the vendor has had **"zero days" to fix the issue,** there are no official patches or mitigations available when the vulnerability is first exploited.

Focusing on zero-day vulnerabilities is vital because **they are exploited before patches exist,** allowing attackers to bypass traditional defenses and gain undetected access to systems. These threats are often used in high-impact attacks, so early detection, threat intelligence, and proactive security are key to reducing risk and preventing serious breaches.

Misconfigurations

Misconfigurations are improper or insecure settings in software, hardware, networks, or cloud environments. They occur when systems are not configured according to security best practices—examples include open ports, default passwords, exposed APIs, or overly permissive access controls.

Misconfigurations are one of the most common causes of cyberattacks. Even secure tools can become vulnerable if set up incorrectly. Attackers actively scan for these weaknesses because they're often easy to exploit and can lead to unauthorized access, data leaks, or full system compromise.

Here are the list of misconfigurations that were detected in the first quarter of 2025.

Sl. No.	CCE-ID	Description	CCSS Base Score
1	CCE-95403-2	A properly configured firewall is one of the most important aspects of overall system security. FirewallD is a complete firewall solution that manages the system's iptables rules and provides a D-Bus interface for operating on them. Starting with CentOS 7, FirewallD replaces iptables as the default firewall management tool.	10
2	CCE-95477-6	Periodic checking of the filesystem integrity is needed to detect changes to the filesystem. Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.	10
3	CCE-95485-9	firewalld. service enables the enforcement of firewall rules configured through firewalld. Ensure that the firewalld service is enabled and running to enforce firewall rules configured through firewalld.	10

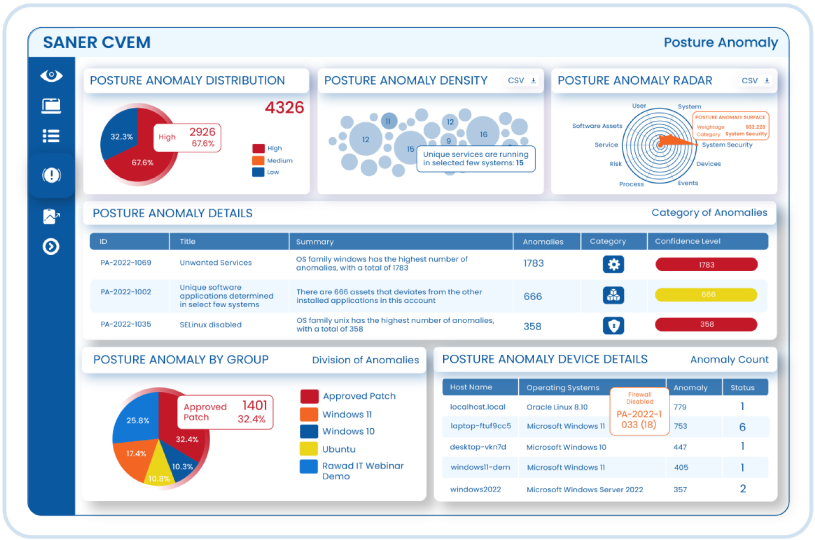
Sl. No.	CCE-ID	Description	CCSS Base Score
4	CCE-95970-0	RHEL 9 must not have the tuned package installed. “Tuned” is a daemon that uses “udev” to monitor connected devices and tunes system settings. Remove it to protect against flaws in its implementation.	10
5	CCE-95971-8	RHEL 9 must not have the iprutils package installed. The “iprutils” package manages IBM Power Linux RAID Adapters. Removing it protects against potential exploitation.	10
6	CCE-23253-8	The ‘Windows Firewall: Domain: Apply local connection security rules’ setting should be configured correctly.	9.8
7	CCE-27072-8	Allow Only SSH Protocol 2 setting should be configured appropriately.	a
8	CCE-38450-3	Specifies encryption level required for RDP connections. High: 128-bit encryption; Client Compatible: strongest the client supports; Low: 56-bit encryption. High is recommended.	9.8
9	CCE-41679-2	Minimum password length policy. Recommend setting it to 14 or more characters to ensure strong, memorable passphrases and defend against brute-force attacks.	9.8
10	CCE-43236-9	Windows Firewall: Domain: Firewall state. Select ‘On’ to enable Windows Firewall with Advanced Security to filter network traffic.	9.8

Posture Anomalies

Security risks don't always stem from known vulnerabilities or external threats—many originate from misalignments within the system itself. These can take the form of disabled security controls, irregular configurations, unauthorized services, or subtle behavioral deviations that may go unnoticed during standard scans. These issues, often referred to as posture anomalies, contribute significantly to the attack surface and are frequently exploited by adversaries looking for low-hanging fruit.

As IT infrastructure grows in complexity across endpoints, cloud environments, and hybrid networks, the need for continuous posture monitoring becomes critical. Traditional security tools may detect known flaws but often fail to surface context-aware or behavior-driven anomalies that evolve over time. Addressing this gap, Saner CVEM's Posture Anomaly Management provides a data-driven approach to uncovering these hidden risks. Leveraging machine learning, statistical analysis, and deviation computation, it monitors thousands of parameters across devices to detect outliers, disabled security mechanisms, and system misconfigurations—before they turn into entry points for attackers.

Know more about how posture anomaly management here:
https://www.secpod.com/saner-posture-anomaly/



Malware Vulnerability Enumeration

While vulnerabilities represent potential weaknesses in software or system configurations, not all of them are weaponized or actively exploited. This is where Malicious Vulnerability Exploits (MVEs) come into focus—they represent vulnerabilities that have been actively leveraged by attackers in the wild, often tied to specific malware campaigns or attack techniques. Unlike the broader pool of CVEs, which includes everything from minor misconfigurations to critical flaws, MVEs narrow the scope to vulnerabilities with real-world exploit activity and adversarial intent.

In the first quarter of 2025, there was only 1 high fidelity attack in the month of March.

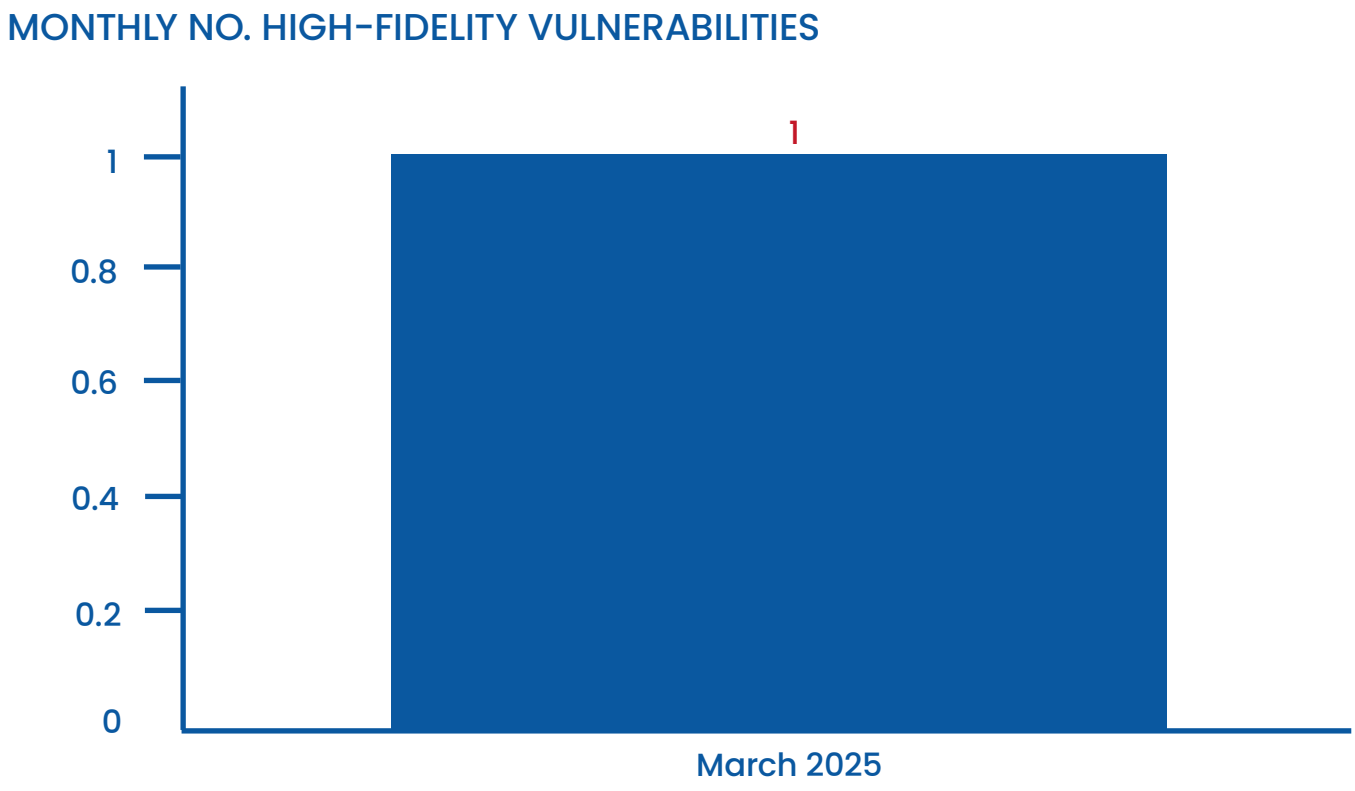


Figure 7: Depicts the vulnerability severity distribution based on CVSS v4 base score

SecPod's Security Intelligence Coverage from January to March 2025

- Total No of CVEs Covered: 5458
- No of Local Checks: 5481
- No of Remote Checks: 270
- Zero-day CVEs covered: 13
- CISA Vulnerabilities Coverage: 55
- Network Device Vulnerabilities: 1504
- Total No of Misconfigurations covered: 1491

CVE Coverage based on platforms:

- Windows - 634
- Linux - 3489
- macOS – 308
- Common Remediation Enumeration (CRE) Coverage: 1712
- Total No of Patches Covered: 1484
- Total No of Third-party applications Patches Covered: 181
- To No of Misconfigurations patches covered: 1304

Benchmarks Coverage

Compliance Benchmark Coverage

Windows Server 2019 STIG Coverage

Ubuntu 23.04 benchmarks revised

Windows Server 2022 STIG Coverage

All AWS Services Coverage

PCI-DSS 321

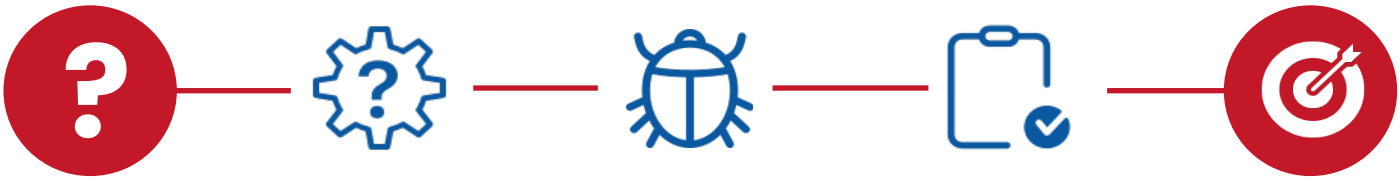
CIS 300,400

STIG, SOC- 2, HIPAA, NIST 800 53

Attack Highlights

1. APPLE CORE MEDIA FRAMEWORK ZERO-DAY EXPLOIT

WHEN	HOW	CVE	RESULT	IMPACT
January 2025	Vulnerability in Core Media Framework via crafted media files.	CVE-2025-24085	Gained kernel-level access to infected iOS devices; used in spyware campaigns.	Targeted attacks on high-profile individuals



2. LAZARUS GROUP STEALS FROM BYBIT CRYPTO EXCHANGE

- **WHEN:** February 21, 2025
- **HOW:** Compromised wallet infrastructure through developer access.
- **CVE:** Not disclosed
- **RESULT:** Theft of ~$1.5 billion in cryptocurrency.
- **IMPACT:** Major financial loss

3. SALT TYPHOON EXPLOITS CISCO IOS XE

- **WHEN:** Dec 2024 – Jan 2025
- **HOW:** Exploited two Cisco zero-days to gain admin access and implant malware.
- **CVE:** CVE-2023-20198, CVE-2023-20273
- **RESULT:** Backdoor access into telecom and ISP infrastructure globally.
- **IMPACT:** Widespread compromise of routers

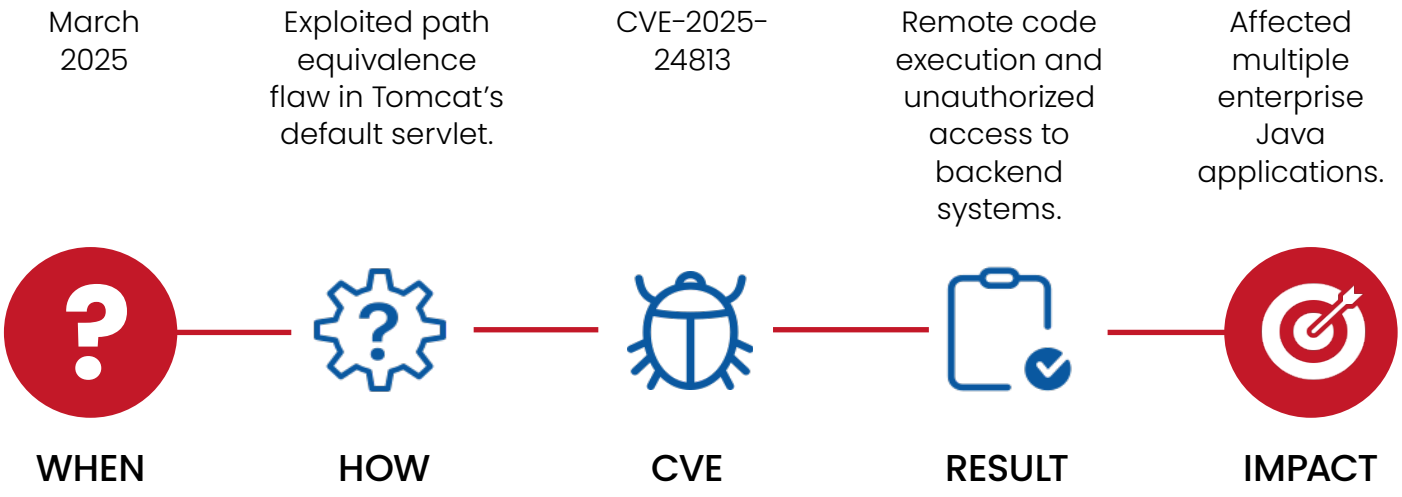
4. UNC5221 ATTACKS IVANTI CONNECT SECURE VPN

- **WHEN:** March 2025
- **HOW:** Buffer overflow in VPN software exploited to deliver TRAILBLAZE and BUSHFIRE malware.
- **CVE:** CVE-2025-22457
- **RESULT:** Remote code execution on thousands of VPN gateways.
- **IMPACT:** Credential theft, persistent access to enterprise networks

5. CODEBREAKERS BREACH BANK SEPAH (IRAN)

- **WHEN:** March 2025
- **HOW:** Internal misconfigurations and legacy systems
- **CVE:** Undisclosed
- **RESULT:** Claimed exfiltration of data from 42+ million customers.
- **IMPACT:** Demanded $42M ransom

6. APACHE TOMCAT PATH EQUIVALENCE EXPLOIT



Since we have covered what happened during Q1, it's time we know what's in store for all organizations in the future.

Vulnerability Prediction 2025

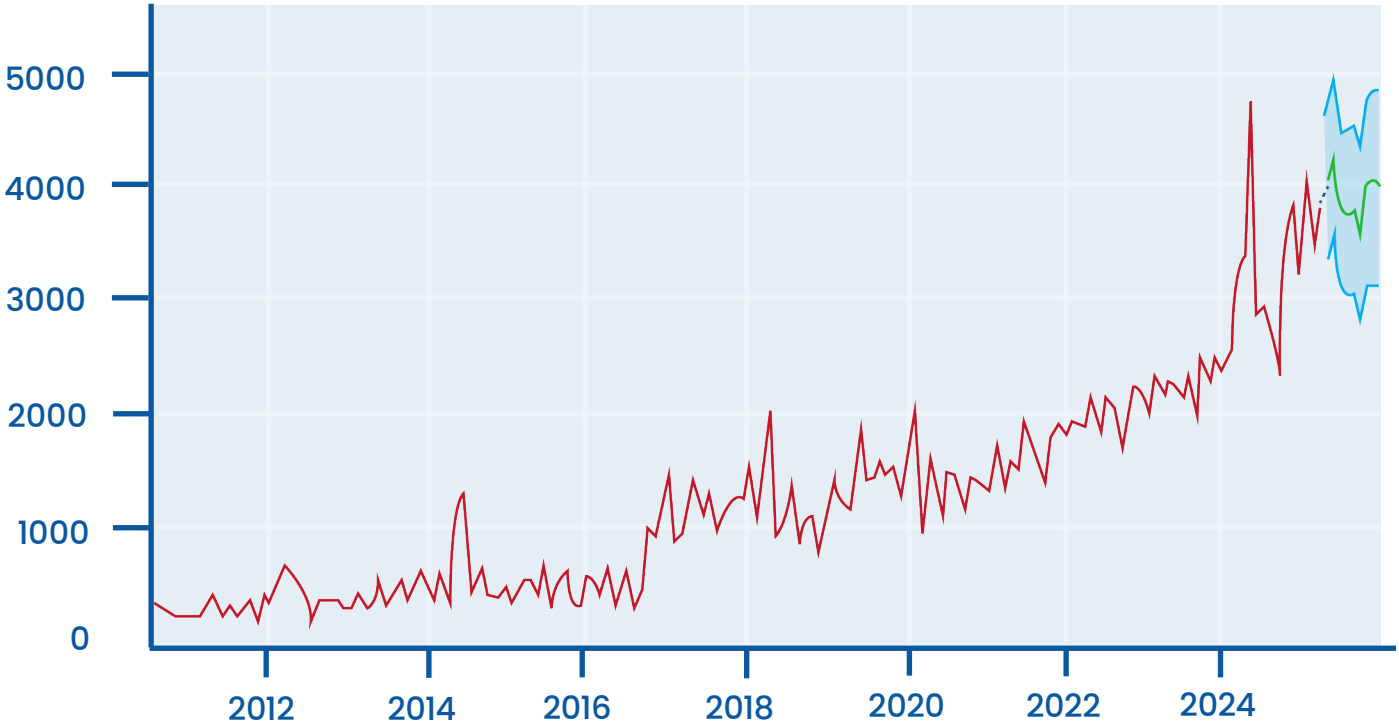


Figure 8: Depicts the vulnerability prediction by SecPod in 2025

Observing the vulnerability trend over the years, from SecPod, we predict over 40000 vulnerabilities in 2025. This prediction is made based on the ARIMA (Autoregressive Integrated Moving Average) model.

Keeping this in mind, we have curated a list of best practices you need to follow to keep your enterprises secure:

1. Implement Strong Access Controls and Identity Management
2. Understand your IT Infrastructure
3. Automate Vulnerability Remediation
4. Test & Deploy Patches
5. Don't just stop at CVEs
6. Perform Regular Security Audits and Assessments

Discover and Eliminate Security Risks with Saner

Saner Platform is a suite of solutions that help organizations establish a strong security posture to preemptively block cyber threats.

The platform includes:

» **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.

With its suite of cutting-edge and comprehensive solutions, SecPod empowers organizations to stay ahead of evolving threats and build a resilient security framework.

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.

Visit us: www.secpod.com

secpod