2026 EDITION

The Cyber Leader's Handbook To **Vulnerability Management**

Vulnerability management is a constant challenge. With the number of documented CVEs continuing to skyrocket year after year, it's hard to know where to focus.

This guide will analyze 2025 CVE data, surface essential insights for optimizing your vulnerability management program, and share key strategies for prioritization.

SIXMAP

Table of **Contents**

SIXMAP

Executive **Summary**

The vulnerability landscape has reached an **inflection point.**

In 2025, over 48,000 CVEs were published—a 750% increase from a decade ago—with this single year accounting for 15.8% of all known vulnerabilities since the CVE program began in 1999. Nearly half of these disclosures were rated High or Critical severity. For security leaders, the message is clear: traditional approaches to vulnerability management are no longer sustainable.

Threat actors have taken notice. According to Mandiant's M-Trends 2025 Report, vulnerability exploitation has become the leading initial access vector, responsible for 33% of all breaches. Attackers are particularly focused on edge devices—firewalls, VPNs, and gateways—with exploitation of these products surging 8x from 2024 to 2025. The very products designed to protect networks have become prime targets, and organizations are struggling to keep pace with remediation.

Yet the data also reveals opportunity. Of the 48,164 CVEs published in 2025, only 165 were added to CISA's Known Exploited Vulnerabilities catalog. This stark contrast demonstrates that effective vulnerability management isn't about patching everything—it's about identifying and prioritizing what truly matters. Smart prioritization, grounded in exploit intelligence and business context, can dramatically reduce risk without overwhelming already-stretched security teams.

This guide examines 2025 CVE data to surface actionable insights for security leaders. We analyze key metrics including CVSS, EPSS, and KEV; explore how threat actors select targets; review high-profile vulnerabilities exploited at scale; and provide strategic frameworks for prioritization. The goal: help security teams focus limited resources where they will have maximum impact on reducing organizational risk.

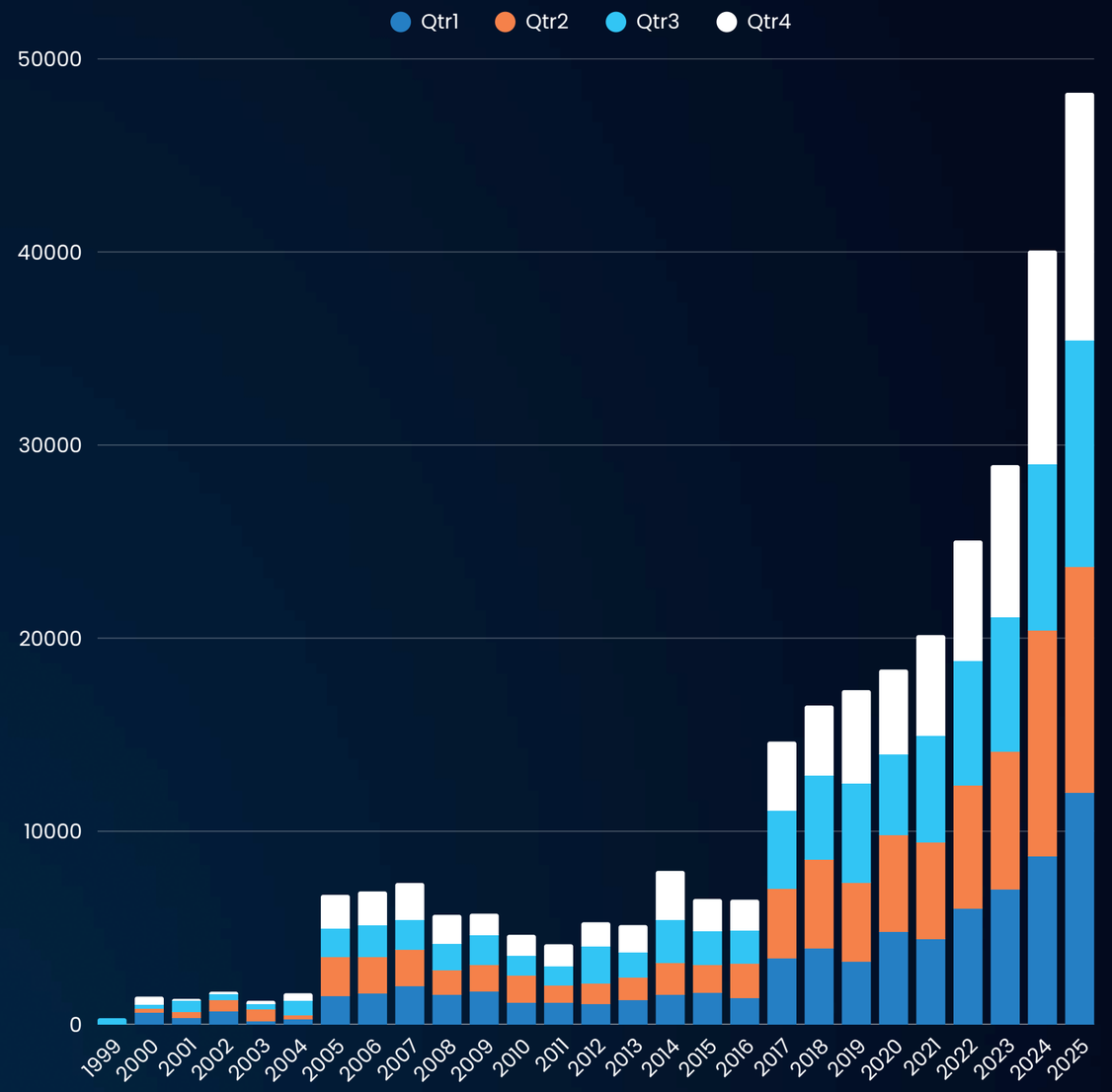
SIXMAP

A Torrent Of CVEs Is Creating Major Challenges

The Common Vulnerability Enumeration (CVE) program was established in 1999 by MITRE Corporation with funding from the U.S. Department of Homeland Security. While the program has delivered immense value to cyber defenders for decades, it now faces mounting challenges from an overwhelming surge in vulnerability disclosures. **In 2025 alone, more than 48,000 CVEs were published—a staggering 750% increase over the 6,494 disclosed just ten years earlier in 2015.** This torrent of vulnerability data is overwhelming security teams and leaving even the most well-resourced organizations struggling to keep pace.

The surge isn't slowing: AI tools are rapidly accelerating the rate at which both researchers and attackers can comb through source code, hunt for weaknesses in applications, and test enterprise software for exploitable bugs. Armed with the knowledge that many security teams are too overloaded to execute rapid remediation cycles, threat actors have focused on launching exploitation campaigns immediately after a severe CVE is published to breach organizations before they have the chance to deploy patches or mitigate the new vulnerability.

Number Of New CVE Records Published Per Year, 1999 to 2025



SIXMAP

Vulnerability: Exploitation Is **On The Rise**

33% of corporate breaches begin with exploitation of a vulnerability in a public-facing application, making it the most common initial attack vector.

Mandiant M-Trends 2025 Report

As CVE disclosures skyrocket, threat actors are increasingly exploiting these exposures. While vulnerability exploitation has been an attack vector for decades, it's experiencing a modern resurgence as the leading initial access method in corporate breaches. According to the Mandiant M-Trends 2025 Report, 33% of all breaches began with exploitation of a vulnerability in a public-facing application—surpassing common techniques like phishing and stolen credentials. The sheer volume of newly disclosed vulnerabilities provides attackers an ever-expanding menu of potential entry points into enterprise networks.

Both nation-state actors and cybercriminals are driving this exploitation surge, though with different motivations. Advanced Persistent Threats (APTs) sponsored by nation-states target vulnerabilities for espionage and intelligence gathering, seeking persistent access to exfiltrate sensitive data over extended periods. Meanwhile, financially motivated ransomware gangs exploit CVEs for immediate monetary gain through data encryption and extortion. Both groups increasingly focus on edge devices—VPNs, gateways, firewalls, and other perimeter products—that provide elevated network access and allow attackers to bypass traditional security controls. These internet-facing systems offer attackers the perfect combination: widespread deployment, direct accessibility, and privileged positioning for lateral movement once compromised.

For security teams, the challenge is compounded by incomplete visibility. Modern enterprises run hundreds or thousands of software applications and dependencies, but many organizations lack accurate inventories of what's actually deployed. They may know they're running Apache or Windows Server generally, but not which specific versions are on which systems, in which locations, or under whose control. When a critical CVE drops, this incomplete visibility turns urgent response into a time-consuming hunt. Add the constant torrent of new CVEs and organizations are left exposed to significant levels of cybersecurity risk.

SIXMAP

Drilling Down On CVE Data From 2025

Vulnerability management presents an immense challenge for enterprise security teams. In 2025 alone, 48,164 CVE records were published to the NIST NVD—more than double the 21,161 vulnerabilities disclosed in 2021, representing a 127% increase in just four years. This single year accounted for 15.8% of all known CVEs dating back to the program's 1999 inception. The severity is equally alarming: 49% of CVEs published last year scored 7.0 or higher, qualifying as High or Critical severity. **With vulnerability exploitation serving as the initial attack vector in 33% of all breaches, the stakes have never been higher.**

So how can organizations move forward and measurably reduce risk? The solution requires three foundational elements: comprehensive asset inventories capturing every software component with precise version information, clear ownership assignment enabling rapid response, and data-driven prioritization focusing remediation on genuine threats. Rather than attempting to patch everything, successful teams identify what matters most by combining asset criticality, exploitability, and threat intelligence. Of the 48,164 CVEs published in 2025, only 165 were added to CISA's Known Exploited Vulnerabilities catalog—demonstrating that smart prioritization, not exhaustive patching, defines effective vulnerability management.

15.8%

of all known CVEs were documented in 2025

#1

initial attack vector in corporate breaches in 2024 was external CVE exploitation (Mandiant)

48,164

new CVE records published to the NIST NVD in 2025

165

CVEs records published in 2025 were added to the KEV in 2025

49%

of all CVEs published in 2025 were assigned a Severity level of High or Critical

32%

of CVEs added to the KEV in 2025 were exploited within 24 hours of disclosure

SIXMAP

CVSS Scores: Base Scores Are Useful But **Limited**

49% of all CVEs published in 2025 were **High or Critical Severity**, meaning they had a **CVSS Base Score of 7 or higher.**

Common Vulnerability Scoring System (CVSS)

DESCRIPTION

CVSS is a 0 to 10 scoring system that quantifies a CVE's severity.

OVERVIEW

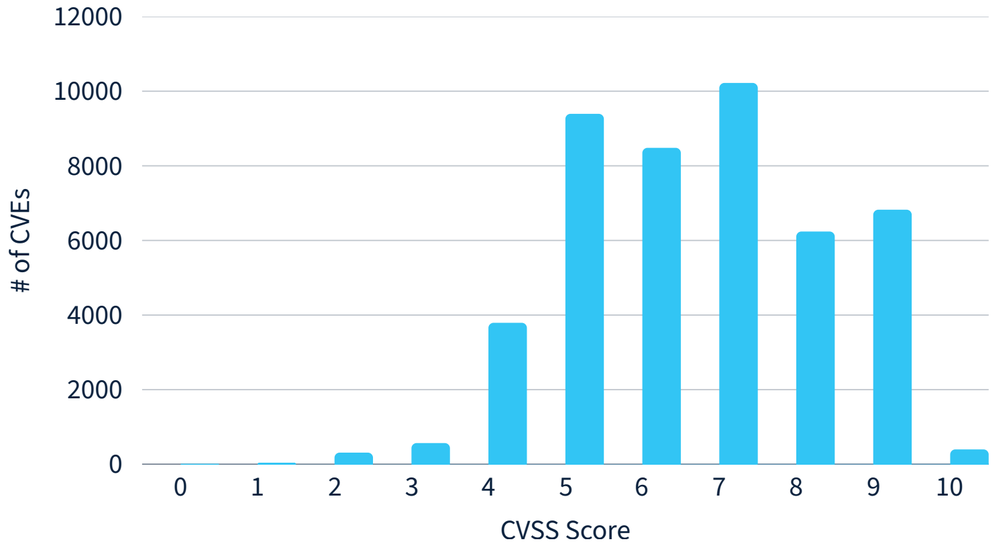
CVSS scores are skewed, with about half of scores >=7 in 2025.

INSIGHTS

CVSS Base Scores are very useful but fundamentally limited, as they don't account for business context or threat intelligence.

CVSS Base Scores provide a standardized severity rating from 0 to 10. However, they don't account for critical context like the importance of the affected asset or whether the vulnerability is actively exploited in the wild. The scoring distribution is also heavily skewed: 49% of all CVEs published in 2025 were rated High or Critical severity (7.0 or higher) While CVSS is an excellent starting point and should absolutely factor into prioritization decisions, it's insufficient on its own. Effective vulnerability management requires layering in additional data, particularly business context and threat intelligence, to focus remediation on urgent risks.

Distribution of CVSS Base Scores For 2025 CVEs



SIXMAP

CWEs: Not All Classes Of Vulnerabilities Are Equal

The **top 10 most common CWEs** were assigned to 25,242 CVEs in 2025, meaning just **1% of all CWEs accounted for 52% of all CVEs published last year.**

Common Weakness Enumeration (CWE)

DESCRIPTION

CWEs identify the type of vulnerability that causes a given CVE.

OVERVIEW

There are 984 CWEs documented and actively assigned to CVEs.

INSIGHTS

Not all CWEs are equal. Some are common and correlate to high severity CVEs while others are obscure and less likely to be a risk.

Common Weakness Enumeration (CWE) is a standardized classification system identifying the types of software weaknesses that lead to vulnerabilities. Multiple CWEs can be assigned to a single CVE, providing deeper context about the flaw's nature. While 984 CWEs exist, their distribution is highly skewed—some appear frequently and correlate with severe CVSS scores, while others are obscure, rarely assigned, and pose minimal risk. This concentration is striking: the top 10 most common CWEs were assigned to 25,242 CVEs in 2025, meaning just 1% of all CWEs accounted for 52% of all published vulnerabilities last year.

Top 5 CWEs In 2025 By Number Of CVEs

SIXMAP

CNAs: A Few Submit Many CVEs, **Many Submit Few**

The top 10 CNAs submitted 34,643 CVE records last year– that's 72% of all CVEs. 122 CNAs, or 25% of all CNAs, submitted zero CVE records throughout all of 2025.

CVE Numbering Authority (CNA)

DESCRIPTION

CNAs are organizations with the authority to submit a new CVE.

OVERVIEW

There are currently 489 CNAs in total worldwide.

INSIGHTS

Many CNAs are also software vendors and the majority of CVEs they submit are related to vulnerabilities in their own products.

CVE Numbering Authorities (CNAs) are organizations authorized to assign CVE IDs and publish vulnerability records within their defined scope. While 489 CNAs exist globally, only 367 contributed CVE records in 2025—meaning 122 CNAs, or 25%, remained inactive throughout the year. The distribution is heavily concentrated: the top 10 CNAs submitted 34,643 CVEs, representing 72% of all records from just 2% of authorized organizations. Critically, many CNAs are also software vendors, and the majority of CVE records they submit affect their own products—a structure that grants vendors significant control over how vulnerabilities in their software are cataloged and disclosed.

Top 5 CNAs In 2025 By Number Of CVEs

Patchstack: **14.6%** 7,016 CVEs

Linux Foundation: **12.3%** 5,924 CVEs

VulDB: **12.3%** 5,916 CVEs

MITRE: **10.9%** 5,248 CVEs

Wordfence: **7.3%** 3,510 CVEs

SIXMAP

CPEs: Common Products Have Higher Volume Of CVEs

The top 10 CPE vendor/product entries had a combined 10,763 CVEs disclosed in 2025, accounting for **22% of all CVE records** published throughout the year.

Common Platform Enumeration (CPE)

DESCRIPTION

CPEs record the vendor, product and version affected.

OVERVIEW

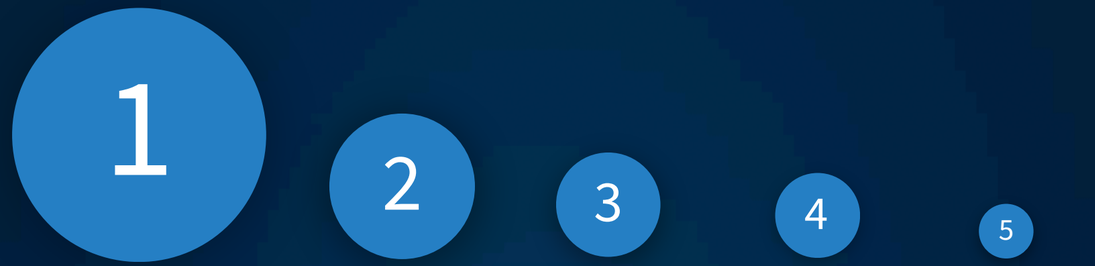
There were over 21,000 unique CPEs with known CVEs in 2025.

INSIGHTS

A single CVE can affect multiple CPEs so it's essential for security teams to know exactly what technologies they have running.

Common Platform Enumeration (CPE) is a standardized naming scheme identifying specific software and hardware products affected by vulnerabilities. Every CVE impacts a precise subset of products—often just a few versions of a single application. In 2025, 21,104 unique CPEs had at least one CVE assigned. Distribution varies dramatically: the Linux kernel alone accounted for 4,175 CVEs, representing 8.7% of all published vulnerabilities. This concentration reflects a crucial reality—widely used enterprise software receives heightened scrutiny from both researchers and threat actors, meaning higher CVE counts often indicate increased attention rather than inherently poor security practices.

Top 5 CPEs In 2025 By Number Of CVEs



SIXMAP

EPSS: Few CVEs Have A High Probability Of **Exploitation**

An EPSS score of 0.01 already ranks at the 96th percentile among all CVEs. **Only 4% of all known CVEs have an estimated chance of exploitation of 1% or greater.**

Exploit Prediction Scoring System (EPSS)

DESCRIPTION

EPSS predicts the chances a CVE will be exploited within 30 days.

OVERVIEW

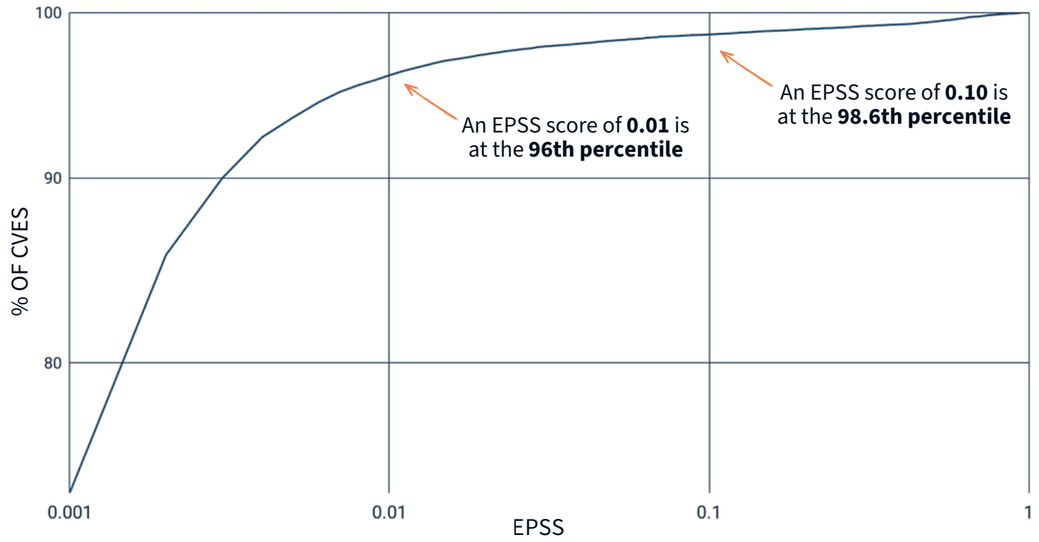
An EPSS score is a probability assigned on scale from 0.00 to 1.0.

INSIGHTS

EPSS scores are skewed, with just 4% of all CVEs published in 2025 assigned an EPSS of 0.01 or higher (at the time of writing).

The Exploit Prediction Scoring System (EPSS) estimates the probability a vulnerability will be exploited within the next 30 days. Unlike static CVSS scores, EPSS is dynamic and updates periodically to reflect current threat landscape activity—a CVE exploited at scale years ago may pose minimal immediate risk today. However, EPSS scores are non-falsifiable, meaning there is no empirical way to test the accuracy of published EPSS scores. Further, EPSS scores are heavily skewed: a score of just 0.01 (1% exploitation probability) places a CVE at the 96th percentile, while 0.1 or higher reaches the 98.6th percentile. This means only 1.4% of all known CVEs have an estimated 10% or greater chance of exploitation in the next month, limiting the efficacy of EPSS in prioritization. Like CVSS, EPSS is useful but not sufficient on its own.

Cumulative Distribution of EPSS for 2025 CVEs



SIXMAP

CNAs & CPEs: The Fox Guarding The Henhouse

CNA / Vendor Name	# CVEs Published In 2025 (as CNA)	# CVEs Affecting Products (as CPE)	# Of Self-Reported CVEs	% Of Self-Reported CVEs
Adobe Systems Incorporated	832	828	828	100
IBM Corporation	606	606	606	100
Oracle	320	322	313	97.2
Qualcomm, Inc.	273	265	265	100
Fortinet, Inc.	958	237	237	100
Apache Software Foundation	218	218	217	99.5
Mozilla Corporation	213	207	207	100
Cisco Systems, Inc.	274	167	165	98.8
Nvidia Corporation	186	99	99	100
SAP SE	212	27	27	100

Many software vendors are also CNAs, authorized to assign CVE IDs for vulnerabilities within their scope. Most vendors maintain responsible disclosure policies requiring researchers to report bugs privately and coordinate announcements, preventing premature announcements that could enable exploitation before patches are available. Many vendor-CNAs self-report all CVEs affecting products they develop, while publishing few (if any) records for third-party vendors' products. This structure means vendors often control the initial CVE submission process for their own software, determining what gets reported and how it's described.

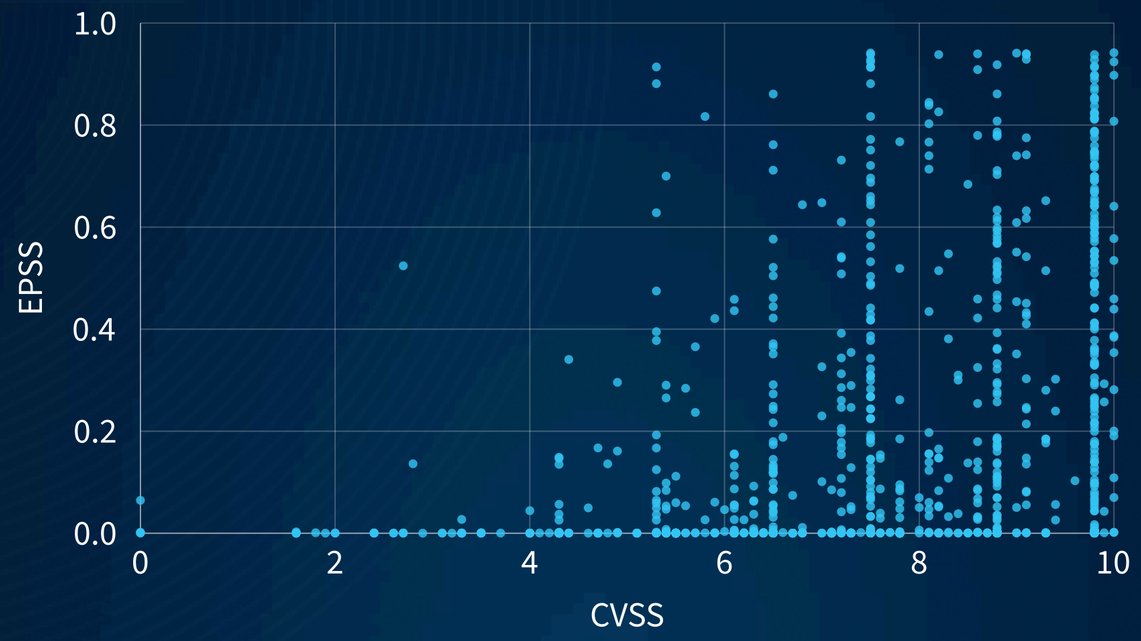
These dynamics position vendor-CNAs as the primary source of vulnerability information about their own products. Since vulnerabilities impacting their software are typically reported to them first—before any CVE reaches MITRE Corporation—vendors control the raw data submitted to the CVE database. Some in the InfoSec community view this as a conflict of interest, as vendors have clear incentives to downplay severity. The data supports this concern: in 2025, 2,692 CVEs received multiple CVSS scores from both vendors and third parties. Vendors consistently rated their own vulnerabilities 0.59 points lower on average than independent analysts.

SIXMAP

Correlation Between **CVSS And EPSS**

CVEs with an EPSS score of **0.01 or higher have CVSS scores that are 22% higher on average.**

Correlation Between EPSS & CVSS For All CVEs Published In 2025



CVSS scores reflect the potential severity of impact if a vulnerability is successfully exploited, but were never intended as risk scores—they lack critical context like asset importance and whether exploitation is occurring in the wild. EPSS, conversely, estimates the probability a CVE will be exploited within the next 30 days, but doesn't assess the severity of that exploitation or organizational impact if systems are compromised. Each metric addresses a fundamentally different question: CVSS answers "how bad could this be?" while EPSS answers "how likely is this to happen?"

Independently valuable, these scores become exponentially more powerful when combined. A statistically significant relationship exists between them: as CVSS scores rise, EPSS scores tend to follow. Among all CVEs published in 2025, the average CVSS score was 7.01. For those with an EPSS score of 0.01 or higher, the average CVSS jumped to 8.50. This correlation reveals threat actor behavior—attackers strategically target vulnerabilities promising severe impact post-exploitation, such as remote code execution capabilities. Understanding this relationship helps security teams predict not just what's severe, but what's actively dangerous.

SIXMAP

KEV: CISA’s Official List Of CVEs Exploited In The Wild

Among the 165 CVEs both published and added to KEV in 2025, a total of **65 CVEs (39.4%) affected products developed by just five major vendors.**

Known Exploited Vulnerability (KEV)

DESCRIPTION

A list of CVEs known to be exploited in the wild by threat actors.

OVERVIEW

There are currently just 1,488 CVEs on KEV, only 0.5% of all CVEs.

INSIGHTS

The KEV list is extremely useful, though it’s widely acknowledged to be incomplete and additional CVEs are exploited.

CISA's Known Exploited Vulnerabilities (KEV) catalog tracks CVEs confirmed as exploited in the wild. While not exhaustive—more vulnerabilities are exploited than KEV captures—it serves as a critical prioritization list since relatively few CVEs ever see active exploitation. The distribution reveals strategic attacker behavior: among 165 CVEs both published and added to KEV in 2025, the average EPSS score was 34.6%, placing them in the 99th percentile. Additionally, 65 of these KEV entries (39.4%) affected products from just five vendors—Microsoft, Ivanti, Fortinet, Apple, and Cisco. This concentration reflects how threat actors selectively weaponize high-value CVEs and exploit them at scale in mass campaigns.

Top 5 CPEs In 2025 By Number Of CVEs

Vendor	# of KEV CVEs in 2025	% of All KEV CVEs in 2025
Microsoft	38	23.03%
Ivanti	7	4.24%
Fortinet	7	4.24%
Apple	7	4.24%
Cisco	6	3.64%

SIXMAP

SIXMAP

How Threat Actors Hunt For Vulnerabilities

Threat actors—both nation-state groups and cybercriminals—primarily target organizations rather than individuals, focusing on vulnerabilities in enterprise software to maximize impact. Widely deployed products are particularly attractive, as a single exploit can compromise hundreds or thousands of organizations simultaneously. Attackers favor CVEs exploitable remotely over networks, especially the internet, eliminating the need for physical access or user interaction. Low-complexity exploits are ideal because they enable partial or full automation, allowing threat actors to launch mass exploitation campaigns that scan for and compromise vulnerable systems at scale with minimal manual effort.

Threat actors employ two primary strategies: discovering zero-day vulnerabilities and weaponizing newly disclosed CVEs. Zero-days represent the ultimate advantage—attackers find, exploit, and breach organizations before vendors or defenders even know the vulnerability exists. Alternatively, attackers monitor CVE publications as a roadmap for targeting. When high-severity CVEs affecting common enterprise software are disclosed, threat actors race to reverse-engineer exploits and launch campaigns immediately. Speed favors attackers: even when patches are available, many organizations take weeks or months to deploy updates, leaving a substantial window of time for full compromise.

SIXMAP

High-Profile CVEs From 2025

CVE ID	Vendor	Product	CWE ID	CVSS Score	EPSS Score	EPSS Percentile
CVE-2025-53770	Microsoft	Sharepoint Server	CWE-502	9.8	0.89607	0.99535
CVE-2025-55182	Vercel	React	CWE-502	10	0.62327	0.98291
CVE-2025-7775	Citrix	Netscaler Gateway	CWE-119	9.2	0.18005	0.94944
CVE-2025-32756	Fortinet	Fortivoice	CWE-121	9.8	0.13781	0.94063
CVE-2025-61882	Oracle	E-Business Suite	CWE-287	9.8	0.78538	0.98991

Vulnerabilities weaponized and exploited at scale share common characteristics. They almost always affect widely used enterprise software and are remotely exploitable over the internet with low complexity, requiring no user interaction. Upon successful exploitation, they deliver severe impact—typically remote code execution granting attackers complete system control. Critically, vulnerable systems are easily discoverable through automated scanning, and exploitation can be fully automated, enabling threat actors to launch mass campaigns that compromise hundreds or thousands of organizations simultaneously with minimal effort.

In 2025, these trends held true as mass exploitation campaigns targeted both new and legacy CVEs. This section examines five high-profile vulnerabilities published and exploited at scale: CVE-2025-53770 (Microsoft SharePoint deserialization), CVE-2025-55182 (React "React2Shell"), CVE-2025-7775 (Citrix NetScaler memory overflow), CVE-2025-32756 (Fortinet buffer overflow), and CVE-2025-61882 (Oracle E-Business Suite authentication bypass). Each achieved CVSS scores between 9.2 and 10.0, with EPSS scores in the 94th to 99th percentile. The following pages detail each CVE's technical characteristics, real-world impact, and strategic significance.

SIXMAP

CVE-2025-55182: React2Shell (React/next.js) RCE

10.0	62%	98th	YES	YES
CVSS Score	EPSS Score	EPSS Percentile	KEV Catalog	Ransomware

CVE-2025-55182, nicknamed "React2Shell," is a CVSS 10.0 pre-authentication remote code execution vulnerability in React Server Components disclosed on December 3, 2025. It affects the react-server-dom-parcel, react-server-dom-webpack, and react-server-dom-turbopack packages in React 19.x, as well as frameworks like Next.js 15.x/16.x.

The vulnerability gained notoriety due to its near-100% exploit reliability, requiring only a single malicious HTTP request with no authentication. Within hours of disclosure, China-nexus APT groups including Earth Lamia and Jackpot Panda began mass exploitation, deploying coin miners, reverse shells, and the SNOWLIGHT/VShell trojans. Given React's presence in approximately 40% of enterprise environments, the blast radius was enormous.

CVE-2025-55182: React2Shell (React/next.js) RCE

DESCRIPTION

Pre-auth RCE vulnerability in React Server Components (RSC)

IMPACTED PRODUCTS

React 19.x, Next.js 15.x/16.x, related RSC frameworks

VULNERABILITY CLASS

CWE-502: Deserialization of Untrusted Data

COMPLEXITY & ATTACK VECTOR

Low Complexity; CVE can be exploited remotely over the Internet

SIXMAP

CVE-2025-7775: Citrix NetScaler RCE

9.2	18%	95th	YES	UNKNOWN
CVSS Score	EPSS Score	EPSS Percentile	KEV Catalog	Ransomware

CVE-2025-7775 is a CVSS 9.2 critical memory overflow vulnerability in Citrix NetScaler ADC and Gateway disclosed on August 26, 2025, with confirmed zero-day exploitation prior to patch availability. The flaw affects appliances configured as VPN, ICA Proxy, RDP Proxy, AAA virtual servers, or certain IPv6-bound load balancer configurations.

This vulnerability is particularly significant because it follows the same configuration prerequisites as previous high-profile NetScaler flaws including CVE-2023-4966 (Citrix Bleed), making it attractive to attackers already familiar with these systems. CISA added it to the KEV catalog the same day with an aggressive remediation deadline. Security researchers noted webshell deployment in observed attacks, with state-sponsored and skilled adversaries being the primary threat actors.

CVE-2025-7775: Citrix NetScaler RCE

DESCRIPTION

Memory overflow enabling pre-auth RCE and DoS

IMPACTED PRODUCTS

NetScaler ADC and Gateway 13.1, 14.1, FIPS editions

VULNERABILITY CLASS

CWE-119: Improper Restriction of Memory Buffer Operations

COMPLEXITY & ATTACK VECTOR

High Complexity; CVE can be exploited remotely over the Internet

SIXMAP

CVE-2025-32756: Fortinet RCE

9.8	13%	94th	YES	UNKNOWN
CVSS Score	EPSS Score	EPSS Percentile	KEV Catalog	Ransomware

CVE-2025-32756 is a CVSS 9.6/9.8 stack-based buffer overflow vulnerability affecting multiple Fortinet products, disclosed on May 13, 2025. Fortinet's Product Security Team discovered it through observed threat activity specifically targeting FortiVoice appliances in the wild.

The flaw allows unauthenticated attackers to execute arbitrary code via crafted HTTP requests containing a malicious hash cookie. Attackers were observed performing network reconnaissance, enabling FCGI debugging to harvest credentials (including SSH logins), and wiping crash logs to cover their tracks. CISA added it to the KEV catalog on May 14, 2025. This marked the eighteenth Fortinet vulnerability to be actively exploited, underscoring the continued targeting of Fortinet infrastructure by threat actors.

CVE-2025-32756: Fortinet RCE

DESCRIPTION

Stack-based buffer overflow via malicious HTTP cookie

IMPACTED PRODUCTS

FortiVoice, FortiMail, FortiNDR, FortiRecorder, FortiCamera

VULNERABILITY CLASS

CWE-121: Stack-based Buffer Overflow

COMPLEXITY & ATTACK VECTOR

Low Complexity; CVE can be exploited remotely over the Internet

SIXMAP

CVE-2025-61882: Oracle E-Business Suite RCE

9.8	79%	99th	YES	YES
CVSS Score	EPSS Score	EPSS Percentile	KEV Catalog	Ransomware

CVE-2025-61882 is a CVSS 9.8 critical pre-authentication remote code execution vulnerability in Oracle E-Business Suite's Concurrent Processing component via BI Publisher Integration, publicly disclosed on October 4, 2025.

First exploitation occurred around August 9, 2025, as a zero-day leveraged by the Cl0p ransomware gang (tracked as GRACEFUL SPIDER) for mass data exfiltration and subsequent extortion campaigns. The exploit chain targets the SyncServlet and XML Publisher Template Manager to achieve unauthenticated RCE. On September 29, 2025, victims began receiving Clop-branded extortion emails. CISA added it to the KEV catalog on October 6, 2025, confirming its use in ransomware campaigns. The targeting of Oracle EBS—which manages critical finance, HR, and procurement data—made this particularly impactful for enterprises.

CVE-2025-61882: Oracle E-Business Suite RCE

DESCRIPTION

Pre-auth RCE in Oracle EBS BI Publisher Integration

IMPACTED PRODUCTS

Oracle E-Business Suite versions 12.2.3 through 12.2.14

VULNERABILITY CLASS

CWE-287: Improper Authentication

COMPLEXITY & ATTACK VECTOR

Low Complexity; CVE can be exploited remotely over the Internet

SIXMAP

CVE-2025-53770: Microsoft SharePoint RCE

9.8	90%	99th	YES	YES
CVSS Score	EPSS Score	EPSS Percentile	KEV Catalog	Ransomware

CVE-2025-53770 is a CVSS 9.8 critical unauthenticated remote code execution vulnerability in on-premises Microsoft SharePoint Server, disclosed on July 19, 2025, with active zero-day exploitation already underway. Dubbed "ToolShell," this flaw is a patch bypass for CVE-2025-49704 (originally demonstrated at Pwn2Own Berlin 2025) and enables insecure deserialization attacks.

When chained with CVE-2025-53771 (an authentication bypass), attackers achieve full unauthenticated RCE. Attackers also steal Machine Keys to forge authentication tokens, enabling persistent access even after patching. Check Point Research observed over 4,600 compromise attempts across 300+ organizations targeting government, telecom, finance, and healthcare sectors in North America and Western Europe. Microsoft initially had no patch available at disclosure, issuing emergency fixes on July 20-22, 2025.

CVE-2025-53770: Microsoft SharePoint RCE

DESCRIPTION

Unauthenticated RCE via insecure deserialization in SharePoint

IMPACTED PRODUCTS

Microsoft SharePoint Server 2016, 2019, Subscription Edition

VULNERABILITY CLASS

CWE-502: Deserialization of Untrusted Data

COMPLEXITY & ATTACK VECTOR

Low Complexity; CVE can be exploited remotely over the Internet

SIXMAP

Security Vendors, Critical CVEs, and **Third-Party Risk**

Only 54% of perimeter-device vulnerabilities were fully remediated by organizations in the past year, while almost half remained unresolved.

Verizon Data Breach Investigations Report 2025

In 2025, threat actors aggressively targeted edge devices—firewalls, VPNs, and gateways designed to protect corporate networks from external threats. The Verizon DBIR noted that zero-day exploits against edge/VPN devices jumped to 22% of exploitation incidents, up from only 3% the year before—an 8x increase. Security vendors bore the brunt of this trend: Fortinet and Cisco each had 8 High or Critical severity CVEs published last year with EPSS scores in at least the 80th percentile, with 6 per vendor added to CISA's KEV catalog. Ivanti fared even worse, with 20 such CVEs and 4 KEV additions throughout 2025.

This trend presents a troubling paradox for security leaders. Organizations invest heavily in security products expecting protection, yet these same vendors are delivering serious vulnerabilities requiring urgent remediation. The companies tasked with safeguarding enterprises have in since cases become primary entry points for threat actors. CISA and international partners have urged software manufacturers to take urgent steps to ship products that are secure by design—guidance that applies especially to security vendors.

These vulnerabilities underscore a broader theme in cybersecurity: third-party risk. Organizations traditionally suffer breaches through insecure vendors storing sensitive data, careless contractors misconfiguring systems, or service providers inadvertently exposing credentials. But there's another dimension: the security of products organizations procure. Thirty percent of data breaches that occurred during the year ended October 31 involved a third party—up from 15% the previous year, according to Verizon. Third-party risk management programs must now assess not just a vendor's organizational security posture, but the security of the products they deliver as well.

SIXMAP

Optimizing Vulnerability Management

Define Your Risk Tolerance

Every security leader must work with executive leadership to understand the organization's risk appetite. Some teams accept significant cyber risk or transfer it through insurance, while others demand reduced risk and increased budgets. Understanding your expected risk threshold and available resources is essential before developing vulnerability management strategy. This foundational alignment ensures security initiatives match business priorities and resource realities.

Keep Complete Asset Inventories

You must know all networks, IP addresses, and domains under your control. Today's complexity—spanning SaaS providers, cloud platforms, third-party partners, and contractors—can make ownership unclear. Maintaining complete inventories with designated asset owners is foundational for defense. Automated discovery tools streamline this process, saving time while ensuring comprehensive coverage of your expanding digital footprint.

Understand Business Context

Beyond basic inventories, security leaders must understand each asset's business criticality. Some assets have minimal impact if compromised and can be deprioritized, while others are mission-critical requiring maximum protection. Assets whose compromise would cause major losses or extended downtime demand prioritized security investments. This context aligns security efforts with organizational priorities.

SIXMAP

Optimizing Vulnerability Management

Know What Software Is Running

Continuous assessment of all assets is fundamental, documenting open ports, services, and running software. Your inventory should include complete CPEs—vendor, product, and version numbers—for every component. This granular visibility enables instant identification of vulnerable systems when CVEs emerge. Rather than scrambling to determine exposure, teams query their inventory and immediately understand impact, accelerating response times and reducing vulnerability windows.

Use Metrics To Prioritize

Data-driven prioritization requires multiple metrics: CVSS scores, EPSS probabilities, KEV inclusion, and business criticality. The key is incorporating relevant data into decisions about which vulnerabilities warrant immediate attention. No single metric tells the complete story—combining CVSS severity, EPSS exploitation likelihood, KEV confirmation, and business context creates effective prioritization frameworks for vulnerability management.

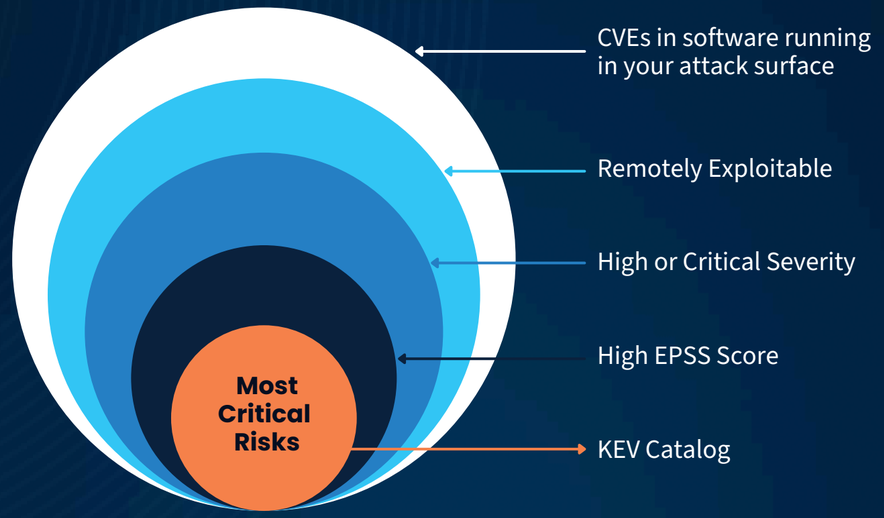
Create Internal Policies For Mitigation

Mature security programs establish SLA-based remediation policies using formulas tied to metrics. For example: KEV-listed CVEs require mitigation within 72 hours; vulnerabilities with EPSS ≥0.5 on critical assets demand remediation within 10 days. Policy specifics must reflect your risk tolerance, available resources, and total CVE exposure. Clear policies eliminate ad-hoc decisions and ensure consistent vulnerability management.

SIXMAP

Strategies For **Prioritization**

Only 0.45% of known CVEs are on KEV, and only 4% have an EPSS of 0.10 or higher. Use these metrics, along with business context of the affected assets, to guide prioritization.



Not all CVEs apply to your organization since you don't run every software product in existence—making up-to-date asset inventories fundamental. Beyond knowing what's deployed, two critical distinctions drive prioritization: CVEs affecting business-critical assets whose compromise would be costly, and CVEs exploitable from the internet versus those requiring internal network access. Internet-facing vulnerabilities on critical assets represent the highest risk, as they're accessible to any attacker globally. Non-critical internal assets, while still requiring eventual remediation, should be deprioritized when resources are constrained and threat actors are actively scanning for exposed vulnerabilities.

Once organizational preparations are complete, leverage external data sources and metrics covered throughout this report. Any CVE on CISA's KEV catalog should be considered urgent and placed atop your remediation priority list—these represent confirmed active exploitation. CVEs with high EPSS scores warrant immediate attention as likely exploitation targets. Beyond these primary indicators, use tertiary metrics like CVSS base scores and exploit complexity to guide prioritization decisions. Other data points such as CWE classifications provide useful context but should play only minor roles in determining a CVE's true risk profile to your specific environment.

SIXMAP

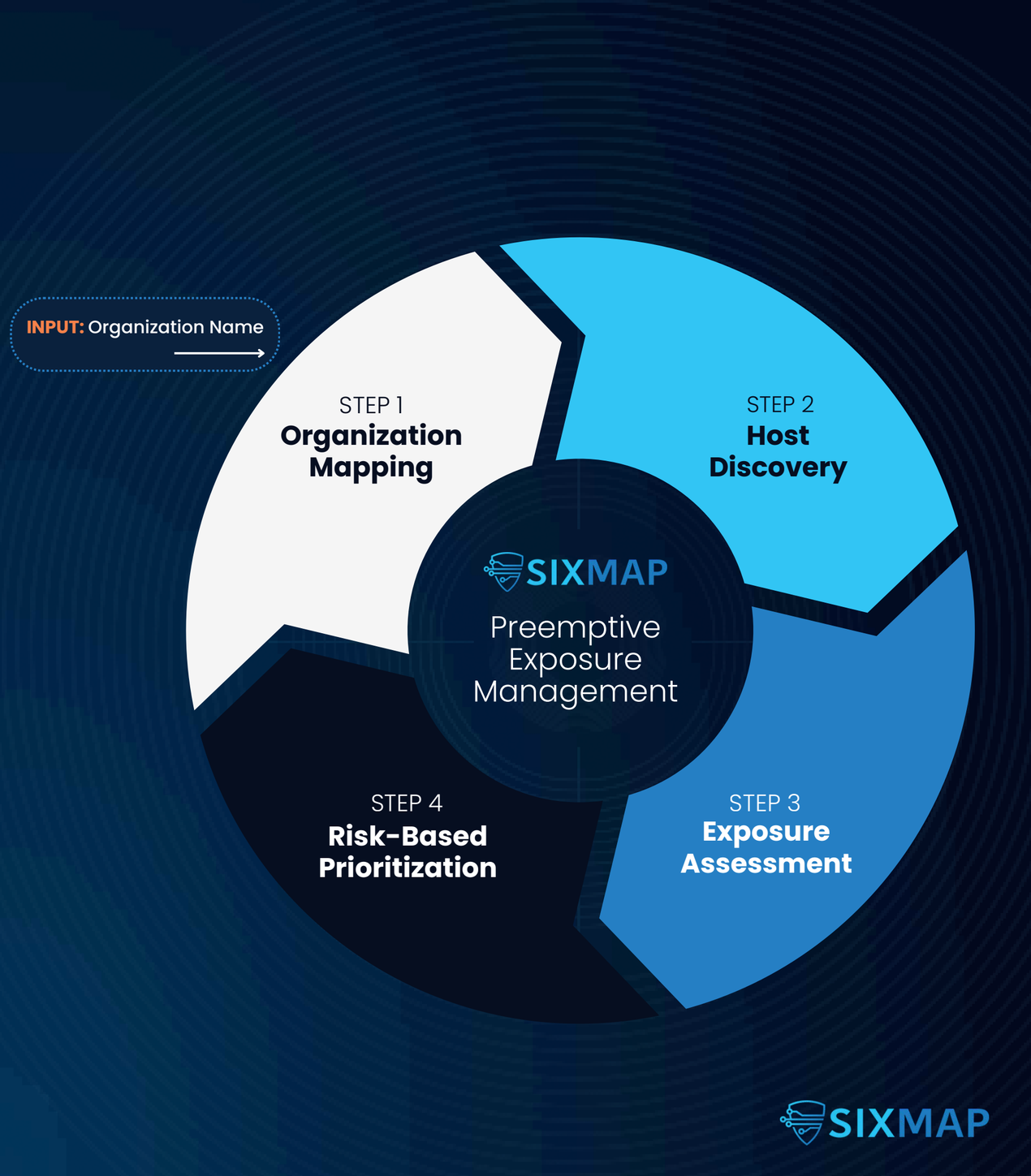
SixMap's Vulnerability Management Use Cases

Save time by automating asset inventory processes.
Gain a centralized view on all the networks, IP addresses, and domains that your organization must defend. Continuously discover your digital estate to detect new assets as soon as they are deployed.

Accelerate remediation when a new CVE is disclosed.
Know which entity within your organization owns each asset so you know exactly who to contact when there's a risk. Quickly understand whether a CVE affects you, which assets are exposed, and who owns the assets.

Continuously assess your assets & quickly detect risks.
Understand your exposures, the services running on each asset, and which vulnerabilities impact your organization. View the diff between any two points in time to see what exactly has changed across the enterprise.

Optimize vulnerability management & reduce cyber risk.
View all the assets vulnerable to a specific CVE, plus threat intelligence on every vulnerability to simplify prioritization. Ensure that the time dedicated to vulnerability management is having a maximum impact on your security.



Conclusion

The 2025 vulnerability landscape presents both a challenge and an opportunity. With over 48,000 CVEs published and nearly half rated High or Critical severity, security teams face an impossible task if they attempt to remediate everything. However, the data consistently shows that only a small fraction of vulnerabilities are ever exploited in the wild—meaning disciplined prioritization can transform an overwhelming problem into a manageable one.

Effective prioritization requires combining multiple data sources. CVSS scores indicate potential severity but lack threat context; EPSS provides exploitation probability but doesn't assess business impact; KEV confirms active exploitation but isn't comprehensive. Used together—and layered with your organization's asset criticality and exposure data—these metrics enable security teams to focus on vulnerabilities that represent genuine risk rather than theoretical concern.

The fundamentals remain essential. Maintain complete asset inventories with precise version information. Ensure clear ownership so the right teams can respond quickly when critical CVEs emerge. Establish policy-driven remediation SLAs tied to risk indicators. And continuously reassess—the threat landscape shifts rapidly, and yesterday's low-priority vulnerability may become tomorrow's mass exploitation campaign. Organizations that build these capabilities will consistently outperform those relying on reactive, ad-hoc approaches.

Vulnerability management at scale requires the right processes, priorities, and tools. **SixMap helps security teams automate asset discovery, accelerate CVE response, and optimize remediation efforts to maximize risk reduction. To learn more about how SixMap can support your vulnerability management program, visit our website.**

SIXMAP

SixMap: Bridging The **Reconnaissance Gap**

Trusted By Security Leaders At The World's Largest Organizations

"Out of thousands of Internet-facing assets, SixMap was able to automatically pinpoint the most pressing vulnerabilities that required immediate action based on quantifying the risk by correlating the threat actors and exploitable vulnerabilities. We're glad they have partnered with AWS to deliver value to their customers."

-Elwin Wong, CISO at Ross Stores

"One of the most powerful cybersecurity capabilities required to operate and defend computer networks ... SixMap Computational Mapping provides public and private sector teams automation for network management and defense so that they can efficiently and effectively operate and defend IPv4-only, dual-stack, and IPv6-only networks."

-United States Army, SBIR 1 Evaluation

"We used to spend days compiling internal and external scans before releasing a new product. Now we just launch and know SixMap will alert us immediately if there's real risk. That gives me high confidence to move faster."

-Douglas Gernat, CISO for the City of Richmond, VA

About SIXMAP

SixMap delivers the most complete and accurate external view of any public or private organization, showing security teams who they are, what they own, and what they must protect. By closing the gap between what security teams monitor and what adversaries find through reconnaissance, SixMap helps customers mitigate risks before attacks occur. Its strategic mapping ensures no assets are overlooked, while advanced technology pinpoints hosts, exposures, and risks with precision. Born out of national defense and deployed to protect some of the nation's most sensitive networks, SixMap now brings military-grade capabilities to public and private organizations to preemptively stop cyberattacks.

BOOK A DEMO

SixMap, Inc. 6731 Columbia Gateway Dr Suite 100 Columbia, MD 21046