CISA Vulnerability Review

Fiscal Years 2024 and 2025

Publication: August 2026
Cybersecurity and Infrastructure Security Agency

DISCLAIMER: This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

The information in this report is being provided "as is" for informational purposes only. CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

This product is not a product of the DHS Office of Homeland Security Statistics or the CISA Statistical Official. Operational data presented in this report reflect trends identified across organizations enrolled in CISA's Cyber Hygiene Vulnerability Scanning service consistent with our commitment to measure and drive risk reduction across our partners.

TABLE OF CONTENTS

Executive Summary

Cybersecurity conversations often focus on high-profile incidents involving nation-state adversaries, ransomware groups, and other sophisticated threat actors. However, most compromises have not relied on advanced techniques. They exploited simple, known software vulnerabilities that remain widespread and persistent in publicly exposed assets. Increasingly, cyber threat actors are using artificial intelligence (AI) to automate all the steps necessary to exploit these vulnerabilities. CISA is publishing the CISA Vulnerability Review to establish a baseline of the vulnerability landscape prior to widespread AI-enabled vulnerability discovery.

In fiscal years 2024 and 2025, most cyber threat activity was not coordinated threat actor groups leveraging zero-day exploits. Instead, it was opportunistic criminals scanning the internet for exposed vulnerabilities created by insecure software. Unfortunately, the production and use of insecure software is still the norm.

Basic security failures enable most compromises. According to the Cyentia Institute's IRIS Ransomware Report,[1] ransomware alone costs organizations an average financial loss of $3.7 million per incident. The report also estimates that organizations have a 10% chance of experiencing a ransomware attack each year.

This publication, the CISA Vulnerability Review, addresses the root causes of insecure software and basic security failures. It draws on CISA and open-source data from fiscal years 2024 and 2025 to provide critical vulnerability insights and tools for software producers and organizations to reduce cyber risk.

Additionally, the review highlights the importance of Secure by Design principles in transforming cybersecurity efforts from reactive to proactive. It also outlines how organizations should prioritize vulnerabilities for action based on exposure status, known exploited vulnerability (KEV) status, exploit automation, and technical impact.

Organizations must shift from reacting to threat actors to fixing the fundamental flaws those actors are known to exploit. Stronger cybersecurity begins with software that is secure by design. It requires prioritization of vulnerabilities and collaboration across industry and government. Finally, it demands leadership attention to understand cyber risk as a business risk, a national security threat, and an impediment to operational resilience.

Organizations must shift from reacting to threat actors to fixing the fundamental flaws those actors exploit.

[1] CISA sponsored the IRIS Ransomware Report's development.

How This Document is Organized

CISA designed this review to help software producers and organizations understand the causes of cyber risk and take meaningful action. It provides a roadmap for reducing vulnerabilities and improving resilience.

The review has two parts: Part 1 primarily addresses software producers and Part 2 primarily end-user organizations seeking to reduce cyber risks.

Part 1: Understanding the Causes of Cyber Risks and the Importance of Secure by Design

This section, which explains the current vulnerability landscape and why most compromises happen, includes:

- A high-level overview of national vulnerability trends.
- An analysis of the common weaknesses that cause most vulnerabilities.
- Secure software development principles every software producer should adopt and what organizations can do in the meantime.

Start with Part 1 to understand the causes of cyber risk.

Part 2: How to Improve Your Organization's Cybersecurity

This section, which focuses on action, includes:

- A simple, prioritized approach to implementing CISA's Cybersecurity Performance Goals (CPGs) 2.0.
- CISA's no-cost resources you can use immediately, including CISA's Internet Exposure Reduction Guidance and Vulnrichment Program.

Use Part 2 for practical steps you can implement today.

How to Apply This Document

Software producers and organizations should:

- Discuss these insights at the highest levels of your organization and consider how the information fits into overall risk planning.
- Align your cybersecurity strategy with CISA's Binding Operational Directive (BOD) 26-04: Prioritizing Security Updates Based on Risk, Secure by Design principles, and CISA's Cybersecurity Performance Goals (CPGs) 2.0.
- Leverage CISA's no-cost resources and participate in collaborative efforts to strengthen national resilience.

PART 1: UNDERSTANDING THE CAUSES OF CYBER RISKS AND THE IMPORTANCE OF SECURE BY DESIGN

Software producers and organizations need a clear view of their cybersecurity strengths and weaknesses to reduce cyber risk. Part 1 of the review outlines the nation's cybersecurity landscape by highlighting patterns in the Common Vulnerabilities and Exposures (CVE) list, the software weaknesses behind them, and the mitigations that software producers can implement to address these weaknesses at the source. It also examines the broader threat environment that shapes today's operational challenges, from emerging attack vectors to supply chain and AI-driven risks. Part 1 concludes with case studies from fiscal years 2024 and 2025, Secure by Design principles, and CISA programs that help software producers and organizations strengthen enterprise security.

Vulnerability Trends and Root Causes

In today's rapidly evolving cyber landscape, software vulnerabilities can quickly shift from latent weaknesses to actively exploited threats. Understanding the weaknesses that give rise to these vulnerabilities is essential to reducing risk at its source. This section examines the most prevalent categories of weaknesses that lead to the vulnerabilities that threat actors are actively exploiting and shows how software producers can address those weaknesses at their source.

CVE Records Overview

Imagine a researcher discovers a vulnerability in a popular application. They alert the software producer, who in this case is a CVE Numbering Authority (CNA).

From there, the clock starts ticking. The researcher and software producer work to fix the issue and create a CVE record. The CNA assigns a unique ID, *CVE-year-number* (e.g., CVE-2026-44228), that becomes the global reference point for tracking the vulnerability from discovery to resolution.

The CVE record also includes:

- A short description of the vulnerability
- Risks and impact
- Affected products and versions
- Weakness type (Common Weakness Enumerations [CWE])
- Links to advisories and mitigation steps

These details help security teams quickly understand what's broken, what's at risk, and how to respond. Public references build trust and point to deeper guidance.

Once published, the record goes into the CVE database, the global vulnerability database for cybersecurity professionals, vendors, and researchers. The CVE program is the primary resource for spotting, prioritizing, and addressing vulnerabilities before threat actors strike.

The CVE Program, launched by MITRE in 1999 and sponsored by CISA, standardizes vulnerability tracking worldwide. CNAs, often software producers, assign CVE IDs and publish CVE records for vulnerabilities within their scope. CVE records are critical tools for defending systems because they provide the clarity that gives everyone—from enterprises to individuals—the insight to stay secure.

Common Weakness Enumerations

CWEs are the global standard for spotting weaknesses in software and hardware. CWEs are not vulnerabilities themselves, but rather flaws in code, firmware, or services that could lead to vulnerabilities. Security professionals use CWEs to find patterns and predict how threat actors could compromise systems. Researchers tag CVE records with CWEs so anyone can trace the vulnerability's root cause.

CNAs and CVE Completeness

The CVE Program has entered its Quality Era, a phase where CVE completeness and consistency is foundational to national cyber defense. A strong CVE record gives cybersecurity teams the insight they need to prioritize and fix vulnerabilities fast. A weak record leaves customers guessing and defenders exposed.

CVE records are critical tools for defending systems because they provide the clarity that gives everyone—from enterprises to individuals—the insight to stay secure.

CISA continues to see preventable gaps in CVEs, such as missing Common Vulnerability Scoring System (CVSS) fields, a lack of CWE attribution, and incomplete descriptions. Those omissions slow triage, undermine security automation workflows, and increase risk across the ecosystem. CVE completeness is not just a best practice, it's a necessity.

Top 10 CWEs Across CVE Records

Analysis of CVE records shows the persistent recurrence of a relatively small set of CWEs. Many of these common weaknesses stem from avoidable coding errors—such as improper input validation and injection flaws.

By incorporating Secure by Design principles that address these simple errors into software development, software providers can prevent entire classes of vulnerabilities and reduce opportunities for exploitation.

FY2024 Findings

In FY2024, the top 10 CWEs accounted for 5.9% of all CVEs. Notably, two of those top 10 were injection flaws. These weaknesses allow threat actors to insert malicious code through trusted input channels—common examples include cross-site scripting (XSS), operating system command injection, and SQL injection. Across the full dataset, injection-related weaknesses made up 10.1% of all CVEs.

FY2025 Findings

The FY2025 picture looks much the same. XSS again dominated the top 10, underscoring the persistence of poor input validation practices that allow threat actors to inject malicious scripts directly into user browsers, which can lead to session hijacking, credential theft, and unwanted redirects. Injection weaknesses overall represented 9.2% of all CVEs. This slight decrease from 2024 is still a substantial share of the total vulnerability landscape.

Address Fundamental Weaknesses

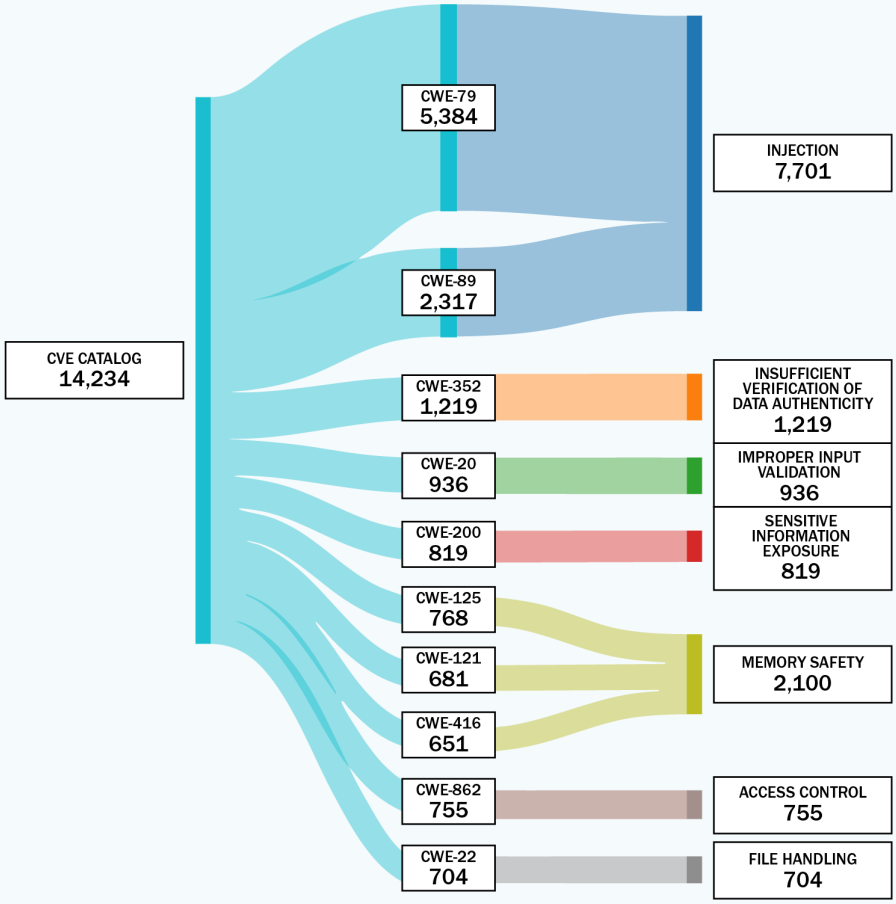
Threat actors continue to succeed, in part, because simple, preventable software weaknesses remain unaddressed. Resolving fundamental issues would eliminate a significant portion of today's most common compromises.

*For a detailed breakdown of the 10 most common CWEs seen across all CVE records, see **Figure 1.1**.*

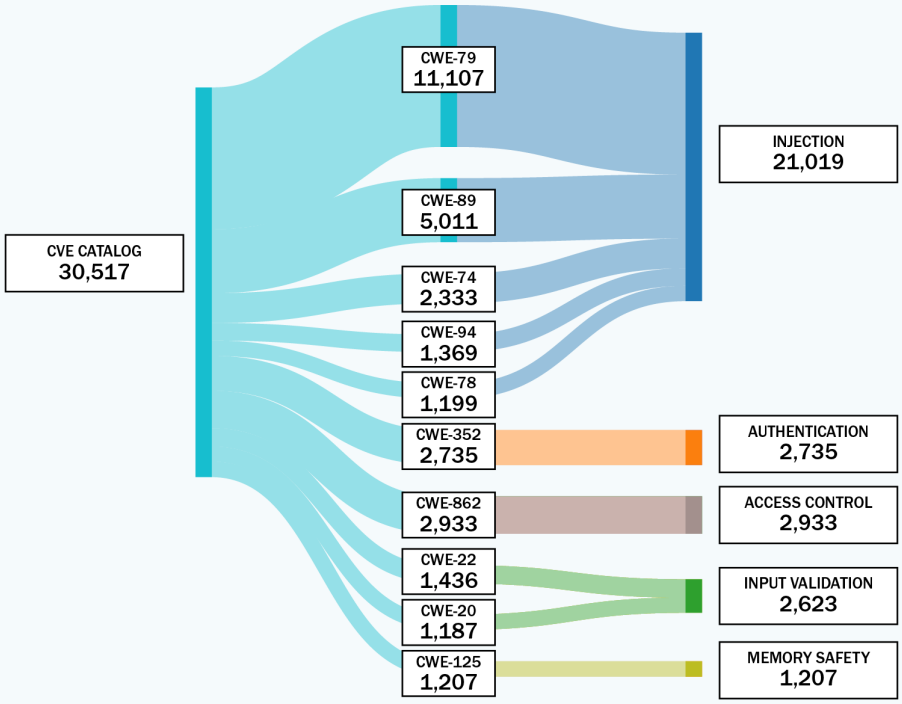
In FY2025, injection weaknesses overall represented 9.2% of all CVEs.

FIGURE 1.1:
FY2024 - 2025 10 MOST COMMON CWEs ACROSS CVE RECORDS

AS OF FY2024



AS OF FY2025



KEVs: Your Patch Playbook

Known Exploited Vulnerabilities

CISA's Known Exploited Vulnerabilities (KEV) Catalog lists high-risk CVEs with confirmed active exploitation in the wild. Organizations should treat KEVs as top priority for remediation and act immediately.

CISA sets remediation deadlines for KEVs that are mandatory for all Federal Civilian Executive Branch (FCEB) agencies and strongly recommended for all organizations. If a KEV is exposed to the internet, organizations should remediate it immediately and investigate for indicators of compromise.

Top CWEs in KEVs vs. All CVEs

Analysis of the top 10 CWEs in the KEV Catalog shows they do not mirror the broader CVE set. Instead of spreading across the full weakness landscape, KEVs cluster tightly around a smaller group of high-impact, reliably exploitable vulnerability types that offer consistent, scalable attack paths.

In FY2024 and FY2025, memory safety and improper input validation weaknesses appear disproportionately in KEVs compared to the full CVE population. For software providers, this finding underscores the importance of addressing the underlying weaknesses that often translate directly into real-world exploitation. By reducing these root causes during software development, providers can help prevent vulnerabilities that are more likely to be targeted by threat actors.

Top 10 CWEs Among KEVs[2]

FY2024 Findings

Memory safety, injection, and improper input validation weaknesses were the most prevalent categories, representing 19.8%, 10.1%, and 8.1% of the FY2024 KEV Catalog, respectively. Six of the top 10 CWEs were within these categories, showing that threat actors repeatedly capitalize on longstanding, well-understood flaws.

Most remaining KEV entries stemmed from file and resource handling issues that continue to recur across software products.

Software providers can reduce this weakness by implementing Secure by Design practices and validating how software handles files and system resources.

FY2025 Findings

Injection weaknesses remained dominant in FY2025 among KEVs. Seven of the top 10 CWEs were in the injection, improper input validation, or file-handling categories, underscoring that many exploited vulnerabilities stem from the same common implementation flaws.

Additional recurring issues included memory safety and access control weaknesses, which persisted across a wide range of modern software offerings.

Counter Threat Actor Strategies

Threat actors use simple, reliable techniques that work across multiple products and environments. Rather than relying on novel exploits, they repeatedly target the same weakness classes that resurface in software. KEVs give threat actors the clearest path to initial access.

Software producers should apply Secure by Design practices and reinforce baseline coding standards to directly reduce compromise. Organizations should prioritize KEV remediation and investigate exposures for indicators of compromise. Fast patching and disciplined software hygiene shut down most exploitation pathways in the KEV Catalog.

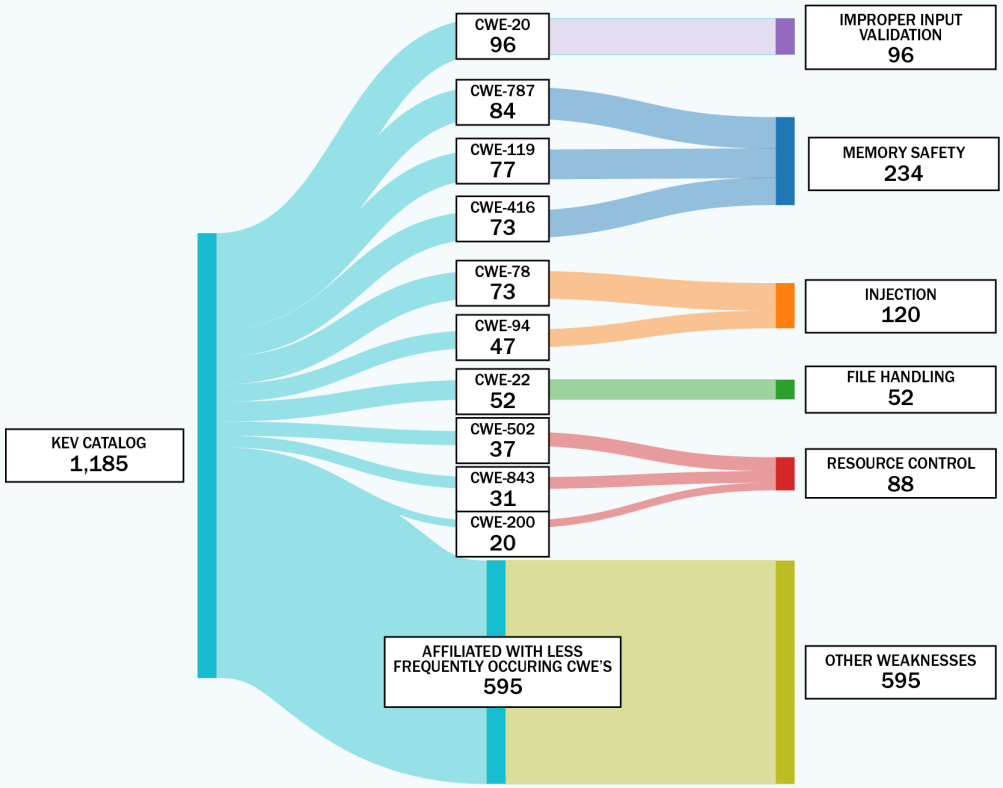
*For further details on the specific CWEs and software weaknesses in the KEV Catalog, see **Figure 1.2.***

Organizations should prioritize KEV remediation and investigate exposures for indicators of compromise.

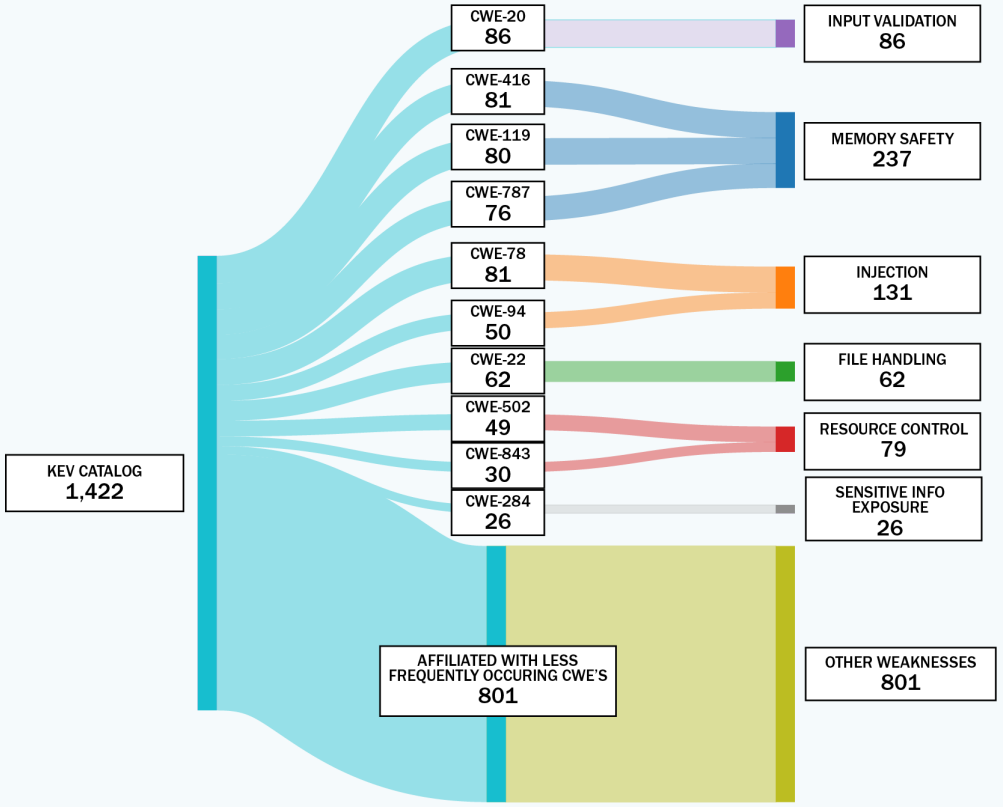
[2] The "Top 10 CWEs Among KEVs" shows the most common weaknesses across all exploited vulnerabilities, while the "Top Six CWEs Driving Compromise" highlights weaknesses currently causing the most real-world breaches.

FIGURE 1.2:
FY2024 -2025 10 MOST COMMON CWEs WITHIN THE KEV CATALOG

AS OF FY2024



AS OF FY2025



How To Address Recurring Software Weaknesses

The following recommendations outline how software producers and organizations can tackle recurring software weaknesses. Each action set aligns with the top weakness categories highlighted in the FY2024 and FY2025 analysis and provides security practices that shut down associated exploitation patterns.

Improper Input Validation

Improper input validation vulnerabilities allow threat actors to manipulate software through unintended inputs, resulting in harmful outcomes for users. They are the most frequent weakness type in both the KEV Catalog and CVE records, which indicates their widespread prevalence and high exploitation potential.

- **Implement strong validation frameworks:** Treat all inputs as untrusted and enforce strict validation.
- **Use the "accept known good" strategy:** Only allow preapproved inputs to minimize security risks.
- **Learn more:** See CISA's Secure by Design Alert: Eliminating OS Command Injection Vulnerabilities.

Improper Input Validations are the most frequent weakness type in both the KEV Catalog and CVE records.

Memory Safety

Memory safety weaknesses occur when software written in non-memory-safe languages, such as C/C++, mishandles memory operations, creating opportunities for exploitation. These weaknesses are prevalent in both the KEV Catalog and CVE records.

CISA encourages software providers to develop memory safe roadmaps to systematically reduce and ultimately eliminate memory safety vulnerabilities from their products.

- **Switch languages**: Reduce use of C/C++ and investigate using others such as Rust, Swift, Java.
- **Create a memory safe roadmap:** See CISA's The Case for Memory Safe Roadmaps.

CISA encourages software providers to develop memory safe roadmaps to systematically reduce and ultimately eliminate memory safety vulnerabilities.

Injection

Injection weaknesses arise when software fails to properly control user inputs, allowing threat actors to inject code through normal data channels without requiring additional mechanisms.

- **Implement strong validation frameworks:** Treat all inputs as untrusted and enforce strict validation.
- **Output encoding:** Properly encode output to prevent misinterpretation when passing it to another component.

File Handling

File handling weaknesses involve improper validation and restriction of file paths, enabling path traversal attacks that grant unauthorized access to sensitive files due to persistent challenges in securely handling user-controlled file inputs.

- **Test regularly:** Run security checks to catch path traversal and input flaws.
- **Enforce least privilege:** Enforce least privilege access by limiting file access to only necessary users.
- **Secure error handling:** Hide paths, usernames, and directory details in errors.

Access Control

Access control weaknesses occur when authorization checks are missing, allowing users to exceed intended privileges and enabling threat actors to escalate access or reach restricted functionality.

- **Apply checks:** Require authorization for all sensitive actions.
- **Centralize control logic:** Consolidate controls to reduce implementation errors and gaps.
- **Test enforcement:** Use reviews and automation to confirm protections.

Mixed-Category Exploits

Analysis shows that many exploited vulnerabilities span multiple weakness categories, with threat actors chaining issues like input-validation failures and access control gaps, highlighting the interconnected nature of software weaknesses.

- **Patch linked flaws:** Prioritize fixing weaknesses that threat actors commonly exploit together.
- **Build Secure by Design:** Embed security design best practices throughout development.
- **Monitor and test continuously:** Identify and mitigate multi-step exploitation paths.
- **Inquire with software producers:** When purchasing software, organizations should ask about measures in place to address common software weaknesses.
- **Consider manufacturer efforts:** Prioritize vendors that demonstrate proactive efforts to reduce vulnerabilities in their products.
- **Routinely maintain software:** Continuously update software to the most recent version to mitigate avoidable vulnerabilities.

*See **page 22** Secure by Design: Build It In, Don't Bolt It On for more information.*

When Software Weaknesses Become Unacceptable

The recurring weaknesses identified in FY2024 and FY2025 point to deeper, systemic issues in software development. Two MITRE reports, Unforgivable Vulnerabilities (2007) and Stubborn Weaknesses (2023), illustrate the problem: long-recognized software weaknesses continue to appear in new products. These flaws are not new, and their recurrence raises a broader question about their long-term acceptability. The next section examines data on weaknesses that persist despite years of industry awareness.

Stubborn Weaknesses

From 2019 to 2025, MITRE monitored the CWE Top 25 Most Dangerous Software Weaknesses and found that 18 appeared every year. MITRE refers to these as "stubborn weaknesses," a consistent signal that certain flaw types do not just linger; they persist.

FY2024 Findings

In FY2024, "stubborn weaknesses" made up a significant share of both common vulnerabilities and actively exploited ones:

- Seven of the 10 most frequent CWEs on the CVE list (5% of all CVEs) are "stubborn weaknesses." These included: CWE-79 (XSS), CWE-89 (SQL Injection), CWE-416 (Use After Free), CWE-352 (Cross-Site Request Forgery), CWE-20 (Improper Input Validation), CWE-125 (Out-of-Bounds Read), CWE-22 (Path Traversal).
- Seven of the top 10 CWEs in the KEV Catalog (comprising 41.5% of all KEVs) were also "stubborn weaknesses:" CWE-20 (Improper Input Validation), CWE-787 (Out-of-bounds Write), CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer), CWE-416 (Use After Free), CWE-78 (OS Command Injection), CWE-22 (Path Traversal), CWE-502 (Deserialization of Untrusted Data).

- Three appear in the top five KEVs, demonstrating how reliably these weaknesses translate into real-world exploitation: CWE-20 (Improper Input Validation), CWE-22 (Path Traversal), and CWE-78 (OS Command Injection).

Seven of the top 10 CWEs in the KEV Catalog (comprising 41.5% of all KEVs) were also "stubborn weaknesses."

FY2025 Findings

The FY2025 data shows a similar pattern:

- Seven of the top 10 CWEs remain "stubborn weaknesses." Of those seven, the five that appear in our dataset are: CWE-78 (OS Command Injection), CWE-89 (SQL Injection), CWE-20 (Improper Input Validation), CWE-125 (Out-of-bounds Read), CWE-22 (Path Traversal).
- Across FY2024 and FY2025, 41.5% of KEVs map to "stubborn weaknesses," proof these flaws persist in injection, input handling, memory safety, and file access.

Unforgivable Vulnerabilities

MITRE's 2007 work on "unforgivable vulnerabilities" adds further weight to the issue. According to MITRE, a vulnerability is considered "unforgivable" when:

- It stems from a common, well-documented mistake.
- The attack path is obvious.
- The exploit is simple.
- Threat actors can find the flaw in minutes.

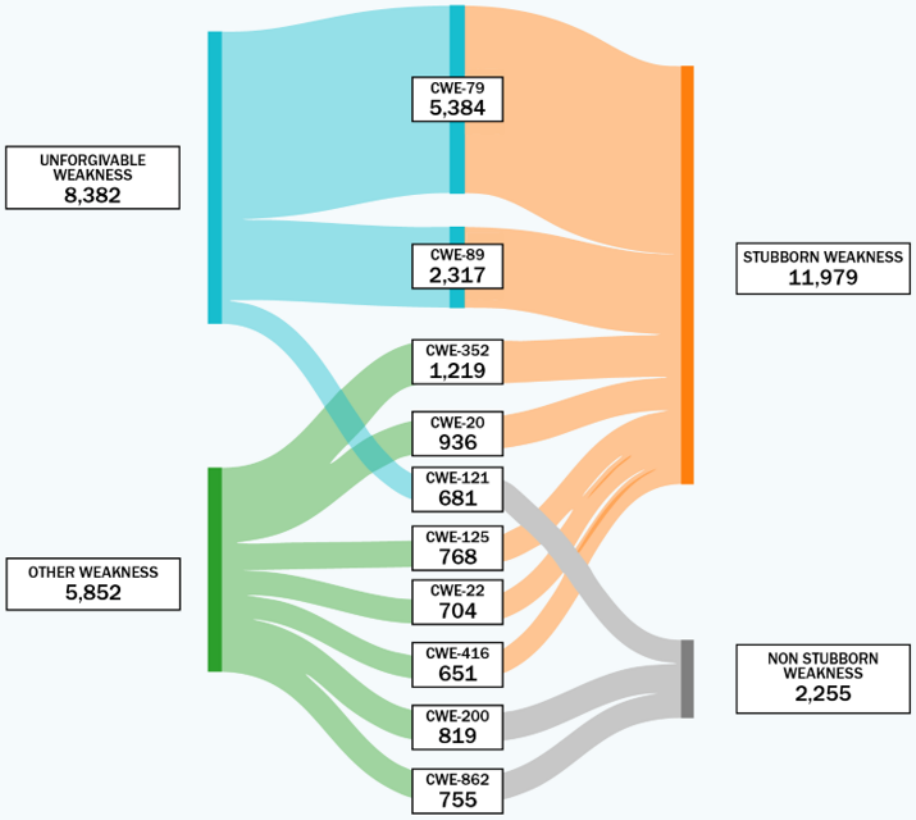
By those standards, **three of today's top 10 CWEs would have been considered "unforgivable" nearly two decades ago**. Their persistence today illustrates that the problem is not technical complexity: it is organizational culture, developer workflows, and systemic gaps in Secure by Design adoption.

For further details on the specific CWE mappings of CVEs and KEVs to MITRE's "stubborn weaknesses" and "unforgivable vulnerabilities," see ***Figures 1.3 and 1.4.***

Three of today's top 10 CWEs would have been considered "unforgivable" nearly two decades ago.

FIGURE 1.3:
FY2024 - 2025 CWE CATEGORIES IN CVES: STUBBORN VS UNFORGIVABLE AND OTHER WEAKNESSES

AS OF FY2024



AS OF FY2025

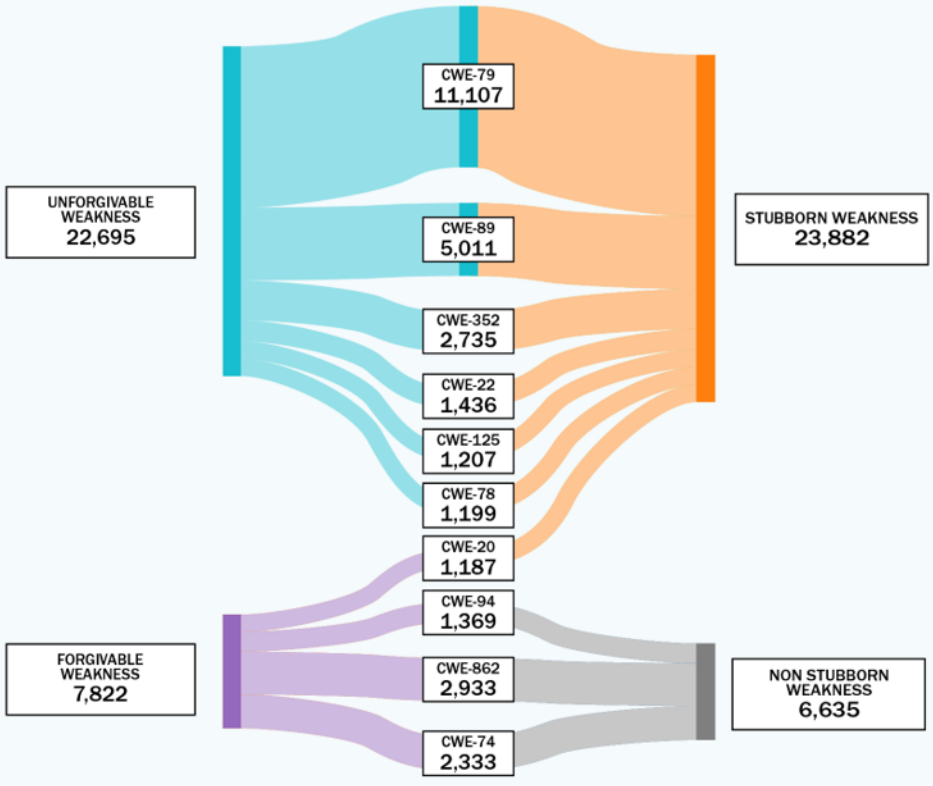
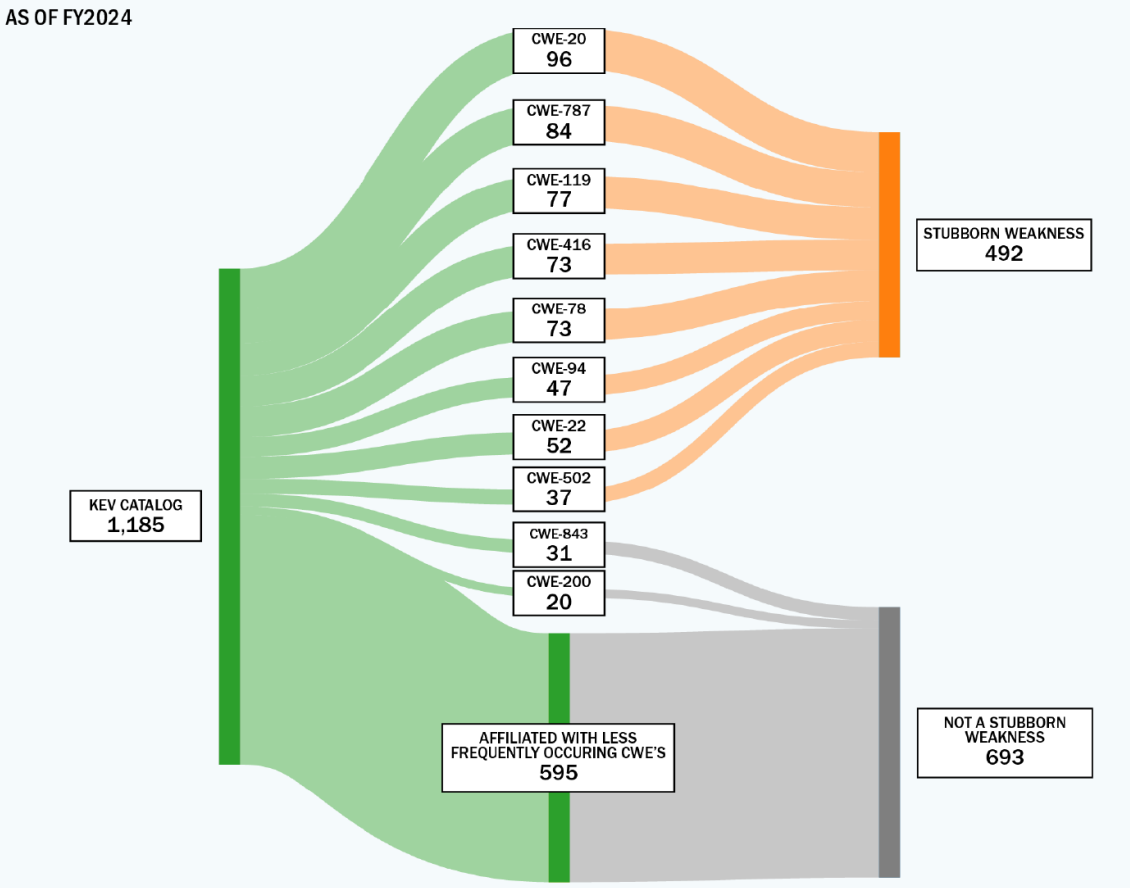
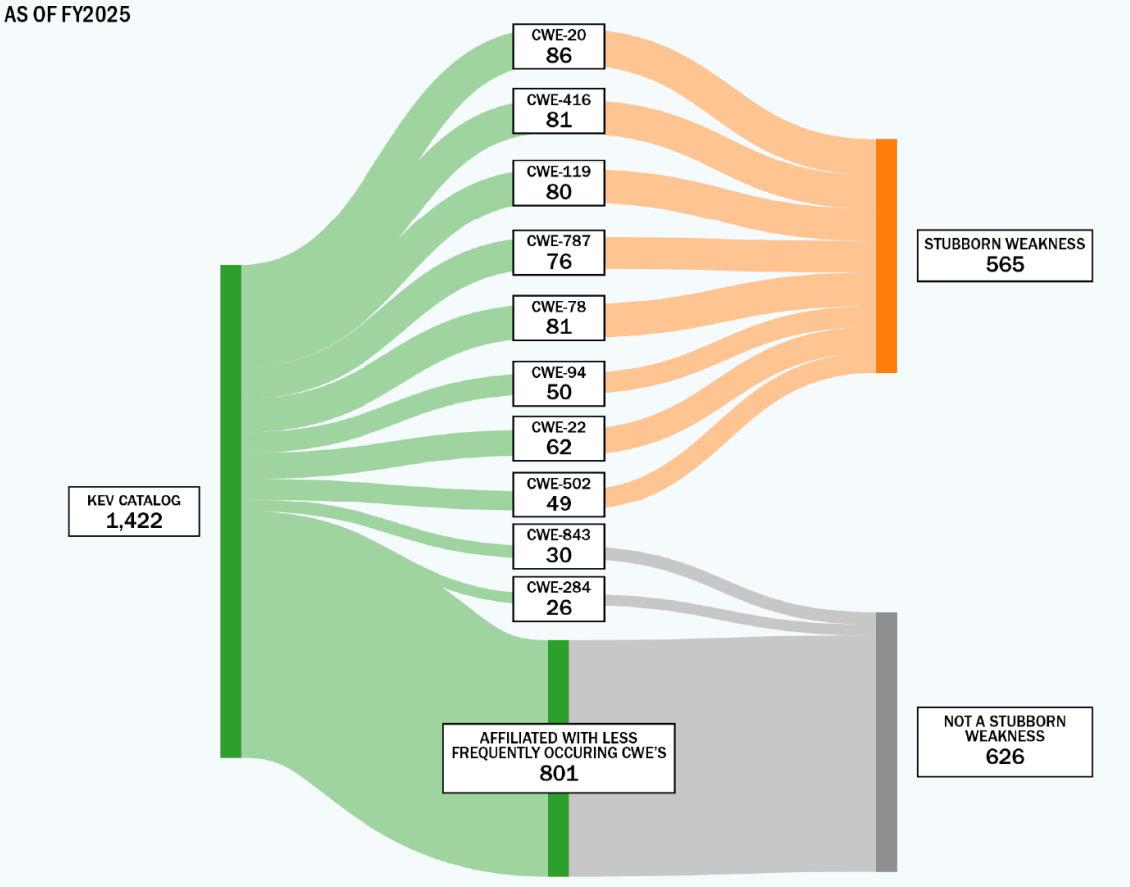


FIGURE 1.4:
FY2024 - 2025 MOST FREQUENTLY EXPLOITED CWEs IDENTIFIED BY CISA RVA ASSESSORS





Insights From Risk and Vulnerability Assessments (RVAs)

These systemic weaknesses show up beyond CVE and KEV data; they surface in hands-on assessments as well. CISA's Risk and Vulnerability Assessments (RVAs) offer a real-world view of how these flaws behave in operational environments, including cyber-mature organizations. The RVA assessments consistently identified the same "stubborn weaknesses" and "unforgivable vulnerabilities" that dominate CVEs and KEVs. From FY2024 to FY2025, improper input validation and memory-safety weaknesses, most frequently CWE-20, remained the most reliable entry points across assessed environments.

FY2024 RVA Findings

- **CWE-20 remains at the forefront:** Improper input validation was the top attack vector.
- **Injection flaws are fading in mature organizations:** Cyber-mature organizations have mostly eliminated injection bugs, forcing assessors to pivot to other avenues.
- **Memory safety is still a major exposure:** Cyber-mature organizations improved, but less mature organizations remain susceptible to memory safety issues.

FY2025 RVA Findings

- **Injection flaws are pervasive**: Command, SQL, and code injection drove most KEVs, showing that input handling and trust boundaries remain unreliable.
- **Memory safety is unevenly improving:** Cyber-mature organizations show progress; less mature ones lag far behind.
- **Stubborn weaknesses persist:** Many top exploited CWEs match MITRE's "stubborn weaknesses," signaling systemic gaps.

__Figure 1.5__ breaks down the 10 most exploited CWEs identified during CISA's RVAs by software weakness type.

RVA assessments consistently identified the same "stubborn weaknesses" and "unforgivable vulnerabilities" that dominate CVEs and KEVs.

Conclusion

When we stack the CVE list against CISA's KEV and RVA findings, the playbook for threat actors is clear:

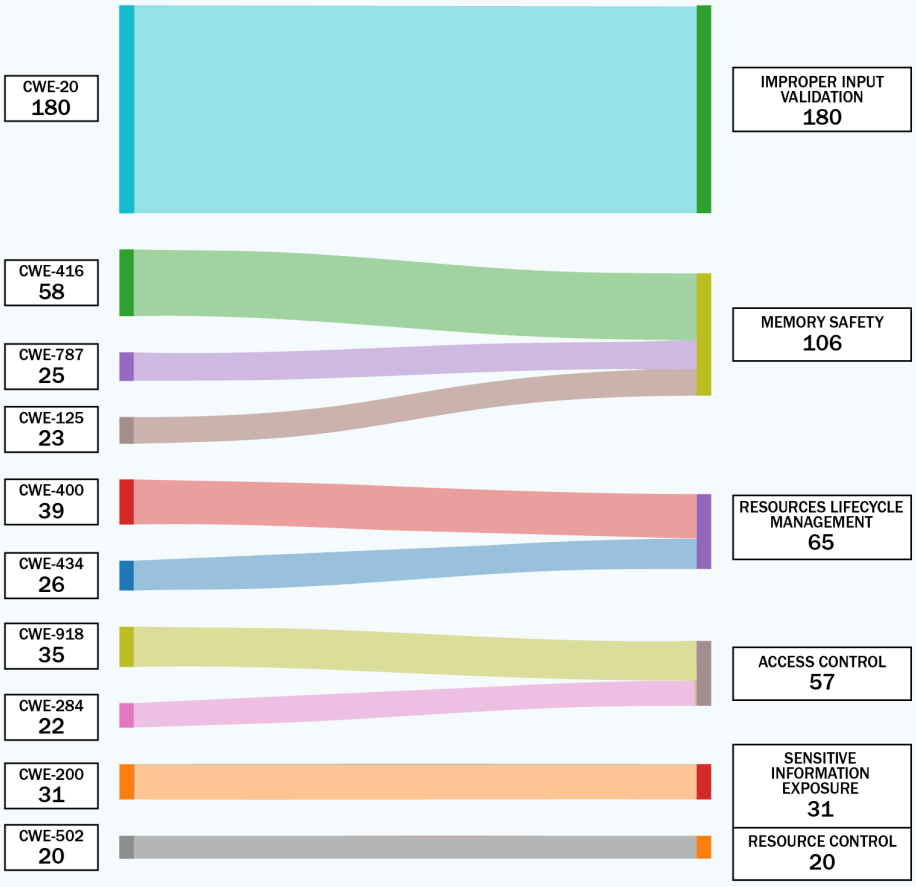
- **Injection flaws:** These constitute a high-volume of the CVE dataset but are rarely successful in cyber-mature environments.
- **Memory safety and improper input validation:** These are the most reliable paths to exploitation, accounting for 19.7% of KEVs in FY2024 and 16.7% in FY2025.

RVAs mirror this pattern. When assessors test cyber-mature organizations, weaknesses tied to memory-unsafe languages and weak validation logic are consistent points of entry. Relying on C, C++, or assembly without modern mitigations leaves defenders exposed.

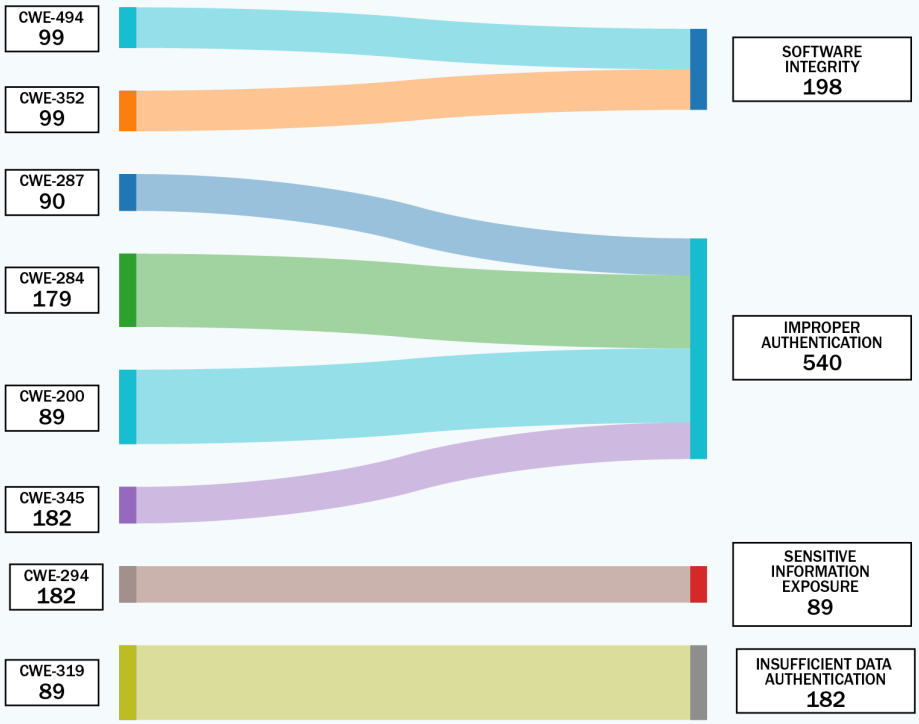
Of the KEV entries, 41.5% are "stubborn weaknesses"—issues documented for years. Some vulnerabilities considered "unforgivable" in 2007 persist in 2025. Whether driven by constraints, resource limitations, or cultural resistance, the result is the same: insecure products and predictable opportunities for threat actors. It is critical that organizations prioritize eliminating these core weaknesses to achieve meaningful, durable risk reduction.

FIGURE 1.5:
FY2024 - 2025 MOST FREQUENTLY EXPLOITED CWEs BY CISA RVA ASSESSORS

AS OF FY2024



AS OF FY2025



Cyber Risk Landscape

As systemic software weaknesses continue to drive exploitation, organizations also face a growing set of operational risks. This section expands beyond vulnerability classes to examine the broader threat landscape, including active attack vectors, technologies introducing new exposures—from the software supply chain to AI—and the organizational gaps that complicate mitigation.

CISA's Cyber Risk Prioritization

This section highlights patterns in the cyber vulnerability landscape and a major shift in how CISA prioritizes risk. For years, CISA treated Common Vulnerability Scoring System (CVSS) scores as the primary decision metric. But CVSS scores are insufficient: they reflect theoretical severity, not real-world impact. Without context, they can mislead teams, inflating low-risk issues while failing to elevate mission-critical threats.

Furthermore, AI-enabled vulnerability discovery is rapidly increasing the volume of disclosed vulnerabilities, requiring ruthless patching prioritization. To address this challenge, CISA changed how it views and prioritizes risks. New guidance[3] focuses on what matters most: fast, mission-driven vulnerability reduction. Prioritization now hinges on four variables:

1. **Asset Exposure:** Is the vulnerable asset publicly exposed?
2. **KEV Status:** Is the vulnerability, as identified by a CVE ID, on CISA's KEV Catalog?
3. **Exploit Automation:** Is an adversary able to automate all the steps necessary to exploit the vulnerability?
4. **Technical Impact:** Does an adversary gain partial control or total control of the vulnerable asset after exploitation of the vulnerability?

CISA publishes answers to questions 2, 3, and 4 through the Vulnrichment Program established in early 2024. For exposure checks (question 1), organizations can consult existing commercial and government tools (see CISA's Internet Exposure Reduction Guidance). To integrate these questions and their answers, CISA recommends adopting the Stakeholder-Specific Vulnerability Categorization (SSVC) as a key decision-making framework. SSVC enables smarter prioritization, sharper risk reduction, and fewer cycles wasted on low-impact vulnerabilities.

This section uses aggregate data from CISA's Cyber Hygiene (CyHy) Vulnerability Scanning services, which provide one of the clearest windows into national cyber risk trends. CyHy scanning monitors vulnerabilities across U.S. critical infrastructure entities. Enrollment jumped from **8,852 organizations in FY2024 to 10,890 in FY2025**, signaling an increasing awareness. The scans expose common weaknesses in internet-facing IT assets, giving a view of external vulnerabilities.

Note: CyHy does not scan internal systems to maintain scalability, avoid operational disruption, and respect privacy boundaries.

[3] See BOD 26-04: Prioritizing Security Updates Based on Risk.

SSVC IN ACTION

In FY2024 and FY2025, CISA designated 520 CVEs for action across critical infrastructure entities, each reflecting a potential exploitable weakness. To prioritize CVEs effectively, CISA applies its SSVC decision tree, which evaluates real-world contextual risk through five factors: exploitation status, technical impact, automatable exploitation, mission prevalence, and public well-being impact. These factors determine one of four SSVC outcomes:

- **Track:** Low priority. Fix during routine update cycles.
- **Track*:** Low priority. Fix during routine update cycles but also watch for changes to the vulnerability that would move it to Attend or Act.
- **Attend:** High priority. Needs attention beyond routine update cycles. Notify teams, escalate, and patch sooner.
- **Act:** Highest priority. Requires immediate action with leadership engagement and rapid mitigation.

As illustrated in **Figure 2.1**, trends show that fewer vulnerabilities fell under *Act, Attend,* or *Track** in FY2025 than in FY2024, and more fell under *Track*. However, organizations should remain vigilant and take immediate action on vulnerabilities that fall under *Act*.

KEV Remediation Timelines: Progress, but Not Fast Enough

Following improvements in vulnerability prioritization through SSVC, the next challenge is execution, and the data is mixed. Between FY2024 and FY2025, CISA observed meaningful progress: critical infrastructure organizations are patching KEVs faster, and fewer organizations are leaving KEVs exposed beyond the first 30 days (See **Figure 2.2**). This is a step forward, but still short of what current operational pressures demand.

Most organizations continue to miss CISA's recommended remediation timelines, leaving systems unnecessarily exposed. Even with year-over-year reductions in exposed KEV instances, the operational risk remains high. Every delayed patch extends the window of opportunity for threat actors, especially when dealing with KEVs.

Top Six CWEs Driving Compromise

Even with faster KEV remediation, the same foundational software weaknesses continue to drive compromise.

FIGURE 2.1:
Percentage of Exposed Vulnerabilities by SSVC Decisions

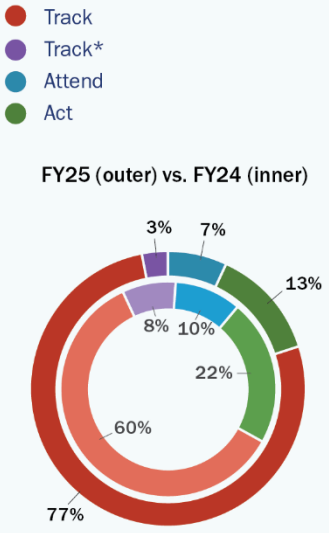
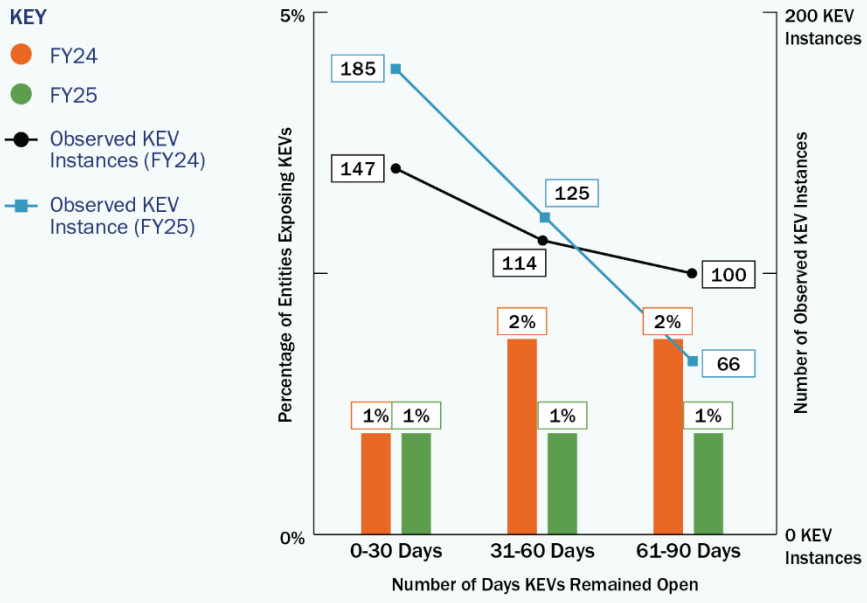


FIGURE 2.2:
Percentage of Critical Infrastructure Entities and Days Exposed to KEVs



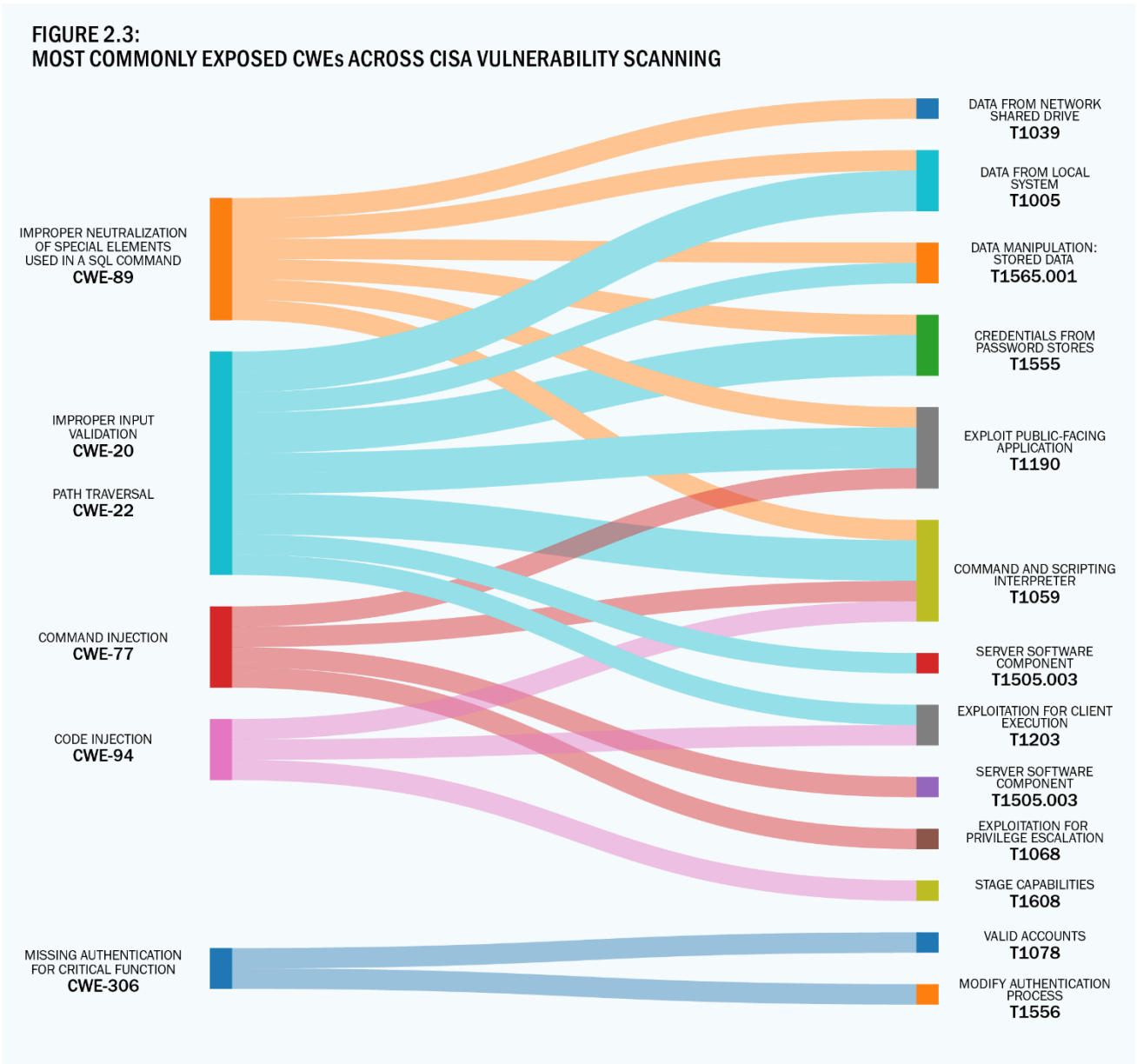
Most KEVs map to six major CWE categories, aligning to 26 MITRE ATT&CK® tactics, techniques, and procedures (TTPs), giving threat actors multiple ways to gain access. The six CWEs are:

- **CWE-89: SQL Injection**: User input isn't sanitized, allowing malicious SQL commands against public-facing apps.
- **CWE-20: Improper Input Validation**: Poor data checks open the door to command execution, credential theft, and data manipulation.
- **CWE-22: Path Traversal**: Allows threat actors to access files outside intended directories, often via web shells or credential stores.
- **CWE-77: Command Injection**: Vulnerable components allow arbitrary commands on the host system.
- **CWE-94: Code Injection**: Threat actors insert and run malicious code within applications.
- **CWE-306: Missing Authentication for Critical Function**: Lack of authentication enables threat actors to take over critical operations.

These CWEs dominate the KEV Catalog for FY2024 and FY2025 and they also appear on MITRE's CWE Top 25 Most Dangerous Software Weaknesses List, showing that threat actors are actively relying on well-known, preventable flaws. Rapid mitigation is essential, as threat actors can exploit each weakness in a variety of ways.

Figure 2.3 provides additional information about the top six CWEs based on CISA Vulnerability Scanning data from FY2024 and FY2025.

FIGURE 2.3:
MOST COMMONLY EXPOSED CWEs ACROSS CISA VULNERABILITY SCANNING



Vulnerable Network Services

Beyond software weaknesses, exposed network services remain one of the simplest paths for compromise. CISA found that 26% of critical infrastructure entities scanned in FY2024 and FY2025 exposed vulnerable network services. These are standard protocols threat actors regularly exploit using techniques mapped to the MITRE ATT&CK® framework.

The use of File Transfer Protocol (FTP) is the most common issue with roughly 18% of scanned entities running FTP servers. FTP lacks encryption and strong authentication. Threat actors intercept credentials sent in clear text, abuse default accounts, and exploit FTP software bugs to steal data or plant malware. In 2025, major flaws in tools like Cleo MFT, CrushFTP, and Wing FTP let threat actors obtain admin access or execute remote code, enabling ransomware and initial access brokers.

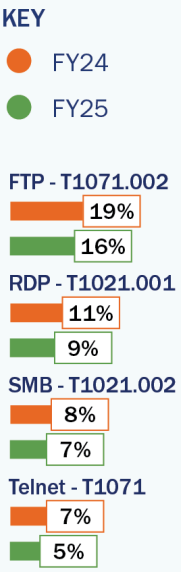
Other high-risk services include:

- **Remote Desktop Protocol (RDP):** A common entry point for ransomware groups. Internet-exposed RDP revealed domains and enabled Chinese-government affiliated cyber actors to conduct lateral movement with BRICKSTORM malware in 2025.
- **Server Message Block (SMB):** Used to spread malware and escalate privileges. In October 2025, CISA added CVE-2025-33073 to the KEV Catalog after active exploitation of a critical SMB flaw.
- **Telnet:** Outdated and unencrypted but still common on legacy and Internet of Things (IoT) devices. In January 2026, CISA added CVE-2026-24061 to the KEV Catalog for a Telnet bug granting unauthenticated root access.

These services are open doors for threat actors. Organizations should disable unnecessary unsecure services and implement strict security controls for necessary services including encryption and strong authentication.

Figure 2.4 provides information about the prevalence of vulnerable network services among critical infrastructure entities.

FIGURE 2.4:
Percentage of Critical Infrastructure Entities Vulnerable Network Services* Mapped to MITRE ATT&CK®



*Vulnerable Network Services Identified in BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces

Exposure of Deprecated Protocols and End-of-Support Software and Hardware

In addition to exposed network services, CISA's CyHy scanning results reveal that many critical infrastructure organizations rely on deprecated protocols and end-of-support (EOS) software—conditions that eliminate the possibility of patching and dramatically increase exploitability. Key findings across FY2024 and FY2025 include:

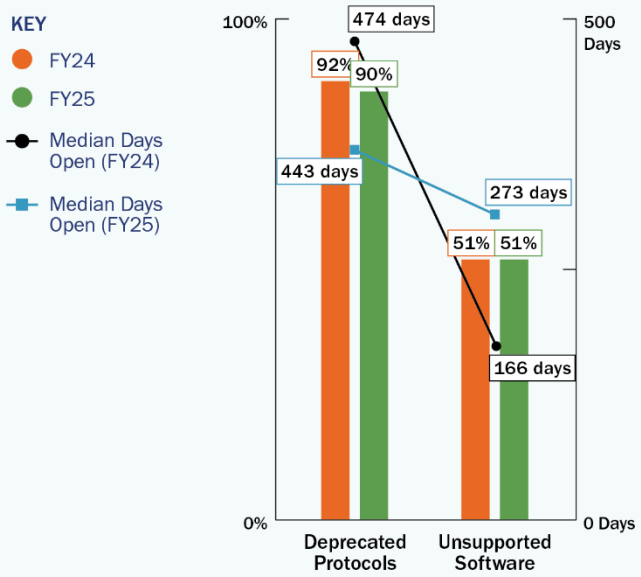
- 51% of scanned entities ran unsupported software linked to over half of KEVs.
- 91% relied on deprecated Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols, often left unsecured for a median of 459 days.

Threat actors exploit these weaknesses—often found in legacy systems—using credential dumping, lateral movement, and interception of sensitive communications, including man-in-the-middle attacks.

Threat actors are also specifically targeting legacy systems which often include EOS edge devices. In February 2026, CISA released BOD 26-02: Mitigating Risk From End-of-Support Edge Devices, directing federal agencies to remove unsupported edge devices from their networks. Without vendor patches, these systems become easy entry points.

Figure 2.5 *provides information about the percentage of scanned entities with deprecated protocols and EOS software in 2024 and 2025.*

FIGURE 2.5:
Deprecated Protocols and Unsupported Software by Median Days Active and Percentage of Entities Exposed



Emerging Technology Risks

As organizations work to eliminate deprecated protocols and EOS technologies, they face a broader challenge: the digital landscape is accelerating, not merely evolving. Rapid adoption of new technologies, growing system interconnectivity, and AI-enabled threats are reshaping the attack surface faster than defenders can respond.

- **Hyperconnected systems** mean one weak link can expose entire supply chains, an interdependence adversaries exploit.
- **AI introduces efficiencies** that threat actors leverage to automate phishing, identify vulnerabilities faster, and scale operations.
- **Legacy IT and unsupported software** remain persistent liabilities, leaving unpatched flaws that become easy entry points for intrusions.

AI: Innovation Meets Exploitation

The United States aims to lead in AI innovation. Sustaining that innovation while protecting the cyber ecosystem requires security built into systems from the start. Two priorities are clear:

1. **Secure AI deployment.** Treat AI systems like any high-risk enterprise software. Incorporate Secure by Design practices informed by common CWEs and CVE trends; follow CISA's cross-sector CPGs; validate models before deployment; and implement controls that promote transparency, robustness, and security.
2. **Defend against AI-powered malicious cyber activity.** Threat actors automate attack paths with AI. Defenders must raise the bar with multifactor authentication (MFA), elimination of entire vulnerability classes, and engineering resilience into systems that integrate AI.[4]

The pace of innovation is accelerating, and security cannot trail behind it. Modernize legacy systems, harden AI implementations, and close off easy pathways threat actors can automate and exploit.

[4] Example techniques include using memory safe languages, applying program verification in continuous integration/continuous development (CI/CD) pipelines, writing well-structured database queries, and designing modular software with least access and least privilege principles.

Case Studies

The following two case studies from FY2024 and FY2025 are real events that exposed gaps and showed how quickly vulnerabilities can turn into compromise. Each case highlights preventable systemic weaknesses and provides lessons learned for organizations to stay ahead.

Case Study #1: When Weak Development Practices Expose the Edge

Poor software development choices don't stay isolated; they expose the very devices meant to defend the enterprise. A recent incident exposed unknown vulnerabilities in edge devices from a major U.S. IT software company. **Edge devices** (e.g., virtual private networks, routers, firewalls) sit at the network boundary. They are the first line of defense and a prime target for exploitation.

Because edge devices control data flow they often serve as the gateway for threat actors. These flaws let **threat actors bypass authentication** and inject commands, facilitating deeper network compromise. During global incident response, investigators confirmed nation-state actors exploited these devices to infiltrate high-value environments.

Government and industry analysis of this incident flagged critical weaknesses, including:

- Authentication bypass
- Command injection risks
- Downstream compromise potential

Analysis of this incident revealed serious vulnerabilities in edge devices that threat actors continue to exploit. The following CWEs are at the root of those vulnerabilities:

Authentication Weaknesses

CWE-287: Improper Authentication

Flaws in authentication protocols enable threat actors to slip past defenses. This weakness ranks on MITRE's Stubborn Weaknesses list.

Injection Flaws

CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

Flaws like SQL injection or command injection where threat actors execute malicious commands, hijack data, and seize control.

Web Application Weaknesses

CWE-918: Server-Side Request Forgery (SSRF)

Threat actors trick servers into sending requests to unexpected hosts, bypassing firewalls and probing internal networks.

Access Control and XML Vulnerabilities

CWE-611: Improper Restriction of XML External Entity Reference

Threat actors use crafted XML files to read local files, expose data, and expand the attack surface.

Privilege Management Weaknesses

CWE-269: Improper Privilege Management

Poor privilege handling gives threat actors unintended control by enabling privilege escalation.

Lesson Learned:

Secure coding at the edge is non-negotiable. Poor development practices turn frontline devices into gateways for threat actors.

Once inside, threat actors leveraged further weaknesses—a stack of software flaws. The incident demonstrates that secure coding isn't optional, and poor development practices put entire networks at risk.

Case Study #2: Unpatched CVEs Fuel Global Surveillance

Since at least 2021, a Chinese government-sponsored cyber threat actor group, known as Salt Typhoon, engaged in a global surveillance campaign by exploiting widely known, unpatched CVEs.

By exploiting such CVEs in internet-facing network devices, the Salt Typhoon threat actor group infiltrated telecommunications, transportation, and military infrastructure across the globe.

According to the joint advisory, Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System, this activity enabled the group to maintain persistent access to victim networks, conduct long-term cyber espionage, and collect sensitive communications and intelligence.

This compromise was effective because edge devices often lack meaningful logging and visibility. Traditional endpoint defenses fail to detect malicious activity. Once inside, threat actors can persist quietly and move with intent.

Preventing compromise requires:

- Router-level hardening
- Telemetry visibility
- Routine threat hunting

Lesson Learned:

If you're not patching KEVs, you're not protected. Unaddressed KEVs give threat actors a clear path to operate at a global scale.

Preventative Secure by Design Approaches: Stop Problems Before They Start

Organizations can prevent the types of failures seen in Case Studies #1 and #2 by applying focused Secure by Design and hardening measures throughout development and operations:

Case Study #1

1. *Safe Software Deployment:* Use extensive testing, controlled rollouts, and failure-anticipation reviews per CISA's Safe Software Deployment Guide.
2. *Eliminate OS Command Injection*: Apply built-in library functions, input parameterization, and limit user-constructed command components.
3. *Eliminate SQL Injection*: Require parameterized queries and prepared statements across all applications.

Case Study #2

1. *Harden Cloud Environments*: Strengthen configurations beyond defaults using CISA's SCuBA Project and vendor hardening guides.
2. *Reduce Attack Surface*: Segment networks, disable unnecessary services, and apply Cross-Sector Cybersecurity Performance Goals (CPGs).
3. *Strengthen Vendor Risk Management*: Require supply chain transparency, SBOMs, and adherence to Secure by Design principles.
4. *Apply General Mitigation Guidance*: Follow the joint Cybersecurity Advisory recommendations and use CISA's Secure by Design Alerts to stay ahead of common pitfalls.

Owning Cyber Risk: Secure by Design

The following Secure by Design approaches demonstrate how failures highlighted in the case studies could have been avoided. Today, consumers and small business continue to shoulder a disproportionate share of the cybersecurity burden. The software producers building the technology we rely on must build security in from the start. This section outlines how software producers and organizations can drive the shift to software that is secure by design.

Secure by Design: Build It In, Don't Bolt It On

Software Producers

CISA urges software producers to reduce the security burden on customers. Build products that are secure at inception rather than relying on constant monitoring, patching, and emergency response.

Software producers need to:

- Automate configuration, monitoring, and routine updates.
- Own security outcomes for their customers.
- Embed security into every phase of design and development.
- Eliminate common vulnerability classes and publish roadmaps for the rest.

CISA recommends producers consult the joint guidance, Safe Software Deployment: How Software Manufacturers Can Ensure Reliability for Customers, to take responsibility for customer security. This approach, which treats security as a core engineering requirement, requires technical discipline and executive buy-in.

End-User Organizations

CISA offers a suite of resources to help organizations build in security from day one, including:

- Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem
- Product Security Bad Practices
- Exploring Memory Safety in Critical Open Source Projects
- The Case for Memory Safe Roadmaps

Critically, the Secure by Demand Guide directs customers on how to use procurement to drive the market demand for Secure by Design products. By establishing clear security requirements before signing contracts, organizations create incentives for software producers to build more secure products. To support these purchasing decisions, the Secure by Demand Guide highlights key questions customers can ask to evaluate whether a product is secure by design and capable of delivering better outcomes:

1. Are security patches simple to install and are automatic updates enabled?
2. Is single sign-on available at no additional cost?
3. Does the product offer MFA or phishing-resistant authentication by default?
4. Have default passwords been eliminated?
5. Which vulnerability classes has the producer already eliminated, and what's the roadmap for the rest?

6. Are security logs included in the base product?
7. Does the software producer provide a machine-readable software bill of materials (SBOM)?
8. Are CWE and Common Platform Enumeration (CPE) fields accurately included for every CVE?

SBOM Adoption: The Future of Software Security

SBOM is now essential to software security and supply chain risk management (SCRM). It acts as an ingredient list for your software, showing every component inside. Without it, finding vulnerabilities is a guessing game.

The conversation has shifted from "*What is an SBOM?*" to "*I have one. How do I use it?*" The answer is automation and interoperability, supported by standardized formats and tools across the supply chain. CISA is driving SBOM adoption across government and industry through initiatives focused on scaling and operationalizing.

SBOM Across the U.S. Government

SBOMs are transforming government cybersecurity by improving supply chain visibility and resilience. CISA is leading this effort across the FCEB, Department of War (DoW), and intelligence community (IC), providing implementation guidance and best practices.

CISA is identifying tools to build a tailored toolkit for generating and consuming SBOMs for internally developed software. Integrating these tools into continuous integration/continuous delivery (CI/CD) pipelines will strengthen software assurance and supply chain security efforts across CISA and the broader FCEB.

SBOM Minimum Elements Update

The SBOM Minimum Elements set the baseline implementation. CISA's 2026 Minimum Elements for SBOM take it further by adding new data fields, practices, and processes to reflect advances since the original 2021 National Telecommunications and Information Administration (NTIA) standard.

Advances in SBOM tools and real-world use are driving these updates. The final version will help agencies and organizations manage software risk more effectively.

Conclusion

Securing the software ecosystem is a shared responsibility. Software producers and end-user organizations both play a critical role.

- **Software producers**: Implement Secure by Design principles, adopt SBOMs, and embrace self-attestation to protect users and build trust.
- **Organizations:** Choose vendors who prioritize security from the start—the fastest path to a stronger security posture.

PART 2: HOW TO IMPROVE YOUR ORGANIZATION'S CYBERSECURITY

The vulnerability trends in Part 1 make it clear that organizations need practical steps they can take now to reduce risk. Part 2 lays out a focused roadmap and no-cost, voluntary CISA services to help organizations strengthen their defenses, prioritize what matters most, and close the gaps threat actors routinely exploit. These are essential actions that raise the security baseline and drive measurable improvements across the cyber ecosystem.

Recommendations

Cybersecurity Performance Goals: Your Priority Playbook

Most organizations do not have unlimited resources and time to lock down their systems. The question is simple: where to start?

CISA's Cybersecurity Performance Goals (CPGs) 2.0 are a focused set of IT and operational technology (OT) practices designed to quickly cut risk and protect U.S. critical infrastructure.

CISA bases the CPGs on real-world threats observed by CISA and its partners as well as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0:

- **Govern** – Set the rules. Establish cybersecurity policies and a clear risk management strategy.
- **Identify** – Know what you have. Understand your assets and the risks that come with them.
- **Protect** – Lock it down. Put safeguards in place to manage risks identified earlier.
- **Detect** – Stay alert. Develop strategies to spot and analyze potential attacks.
- **Respond** – Act fast. Outline what happens when an incident is detected.
- **Recover** – Bounce back. Plan how to restore assets and operations after a disruption.

The CPGs provide organizations:

- **Prioritized essentials.** They are a minimum set of high-impact practices.
- **Maximum impact for investment.** They focus limited resources on actions with the highest impact.
- **Accessible at all levels.** They apply to organizations of all sizes and levels of cyber maturity.

They answer the real questions:

- How do we get started?
- How do we secure both IT and OT?
- Which controls matter most?
- How do we show leadership where to invest?

CPGs are not mandatory, but CISA expects them to become a **standard of care**. They represent an organization's first step toward stronger cybersecurity.

Inside the CPG Design

CISA chose each CPG through a rigorous selection process with input from industry, government, and cybersecurity experts. When NIST released CSF 2.0, CISA updated the CPGs to align with it and the evolving threat landscape, resulting in CPG 2.0.

Every goal had to meet three criteria:

1. **Proven Impact** – Does it reduce risk from the threats and tactics threat actors use most?
2. **Clear and Actionable** – Can organizations understand it and act on it without confusion?
3. **Practical for All Sizes** – Is it financially and operationally achievable, even for small- or medium-sized organizations?

The CISA CPG webpage's visual model shows:

- The goals themselves
- The risks and threat actor tactics they address
- The cost and ease of implementation
- The expected outcomes from implementation
- Support resources and references

Figure 3.1 provides the components of a CPG.

Evaluating Where You Stand

To evaluate how your organization stacks up against the CPGs, start with the **CPG 2.0 Assessment**—a quick, 34-question checkup you can do yourself or with a CISA partner using the Cyber Security Evaluation Tool (CSET) hosted on GitHub. CSET is a Department of Homeland Security desktop application packed with 60+ cybersecurity assessments.

Here's how the process works:

1. The assessment measures your progress toward the latest CPGs.
2. You and your CISA Regional Cybersecurity Advisor (CSA) review the results from the completed assessment and recommended actions.
3. From there, you can enroll in additional CISA assessments or adjust your business plans to strengthen your cybersecurity posture.

Before starting an assessment, CISA strongly recommends an initial conversation with your **Regional CSA**. That discussion sets the stage for your CPG Assessment and future evaluations.

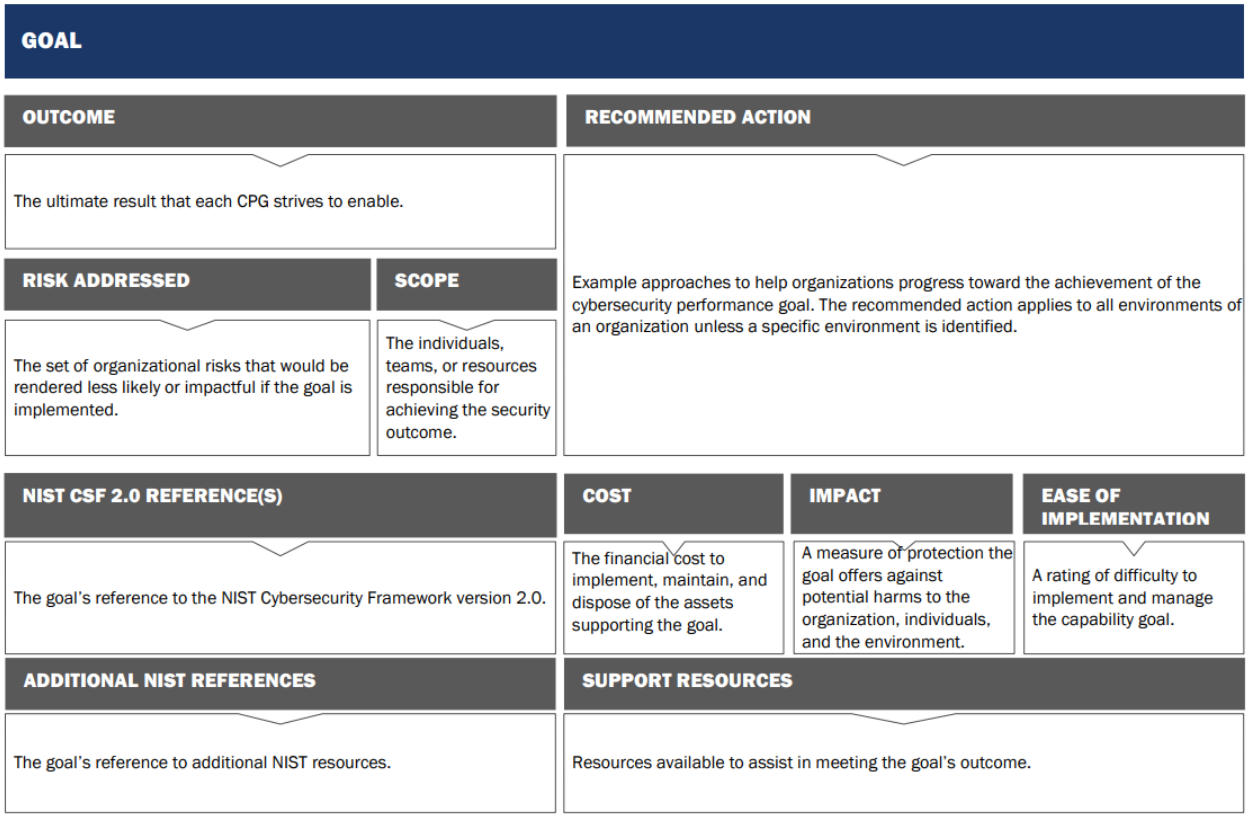


Figure 3.1: CPG Components

CISA's Cyber Risk Reduction Activities and Resources

Getting to a safer digital future takes teamwork across federal, state, local, tribal, and territorial governments, businesses, and nonprofits. CISA is leading the charge with a wide range of activities to reduce risk and a suite of no-cost, voluntary cybersecurity services for organizations nationwide. These services are open to U.S.-based organizations of all sizes and cyber maturity levels. They cover everything from preventing incidents to responding when they happen—because resilience means being ready for both.

Table 1: A Selection of CISA No-Cost, Voluntary Cybersecurity Services

Service	Description	Impact
Cyber Performance Goals (CPGs)	The CPGs are a focused set of IT and OT practices designed to quickly cut risk and protect U.S. critical infrastructure.	Organizations can focus security investment where it matters most. Reduces overwhelm from large frameworks by offering a simplified, outcome-driven list. Improves efficiency of cybersecurity budgets and staffing.
Regional Representatives	Cybersecurity Advisors (CSAs) work directly with organizations in their communities by assessing readiness, strengthening defenses, and responding when attacks happen.	CSAs amplify CISA's mission by bringing cybersecurity expertise directly into communities, improving readiness, reducing risk, strengthening defenses, and enabling rapid, informed response when incidents occur.
Cybersecurity Reporting	CISA issues a multitude of cybersecurity reports that organizations can leverage to enhance their cybersecurity and gain a better understanding of the cyber landscape.	CISA can identify systemic risks earlier, coordinate resources across sectors, and prioritize support to the most affected entities.

Service	Description	Impact
Cyber Hygiene (CyHy) Vulnerability Scanning (VS)	CISA's no-cost VS identifies weaknesses from a threat actor's perspective and provides regular, actionable remediation reports. The service helps organizations proactively close security gaps in their external attack surface, strengthen their overall security posture, and reduce the likelihood of successful compromise.	Organizations enrolled in the CyHy VS service see a 40% reduction in organizational risk and exposure of external vulnerabilities detected in the first year of the service—with many seeing results in 90 days.
Pre-Ransomware Notification Initiative (PRNI)	PRNI provides speedy alerting to organizations in the United States and around the world when early signs of ransomware appear on their networks.	PRNI has saved organizations an estimated $10.5 billion and alerted 71 international governments to compromises in their jurisdictions.
Risk & Vulnerability Assessments (RVAs)	For mature critical infrastructure organizations, CISA provides full RVAs. These on-site penetration tests evaluate an organization's security posture and result in a detailed report outlining weaknesses, risks, and clear actions to address them.	On average, organizations reported a 60% reduction in exposed risks across their networks after completing an RVA.
Coordinated Vulnerability Disclosure (CVD) Program	A key part of CISA's mission to protect critical infrastructure and bolster national cybersecurity. The program reduces risk to essential services by identifying, addressing, and publicly disclosing CVEs.	This collaborative program builds trust, transparency, and a stronger global cybersecurity ecosystem, ensuring the safety of vital infrastructure.

For a comprehensive list of no-cost, voluntary CISA services, visit No-Cost Cybersecurity Services and Tools.

External Service

In addition to the services listed above, CISA encourages organizations to adopt OpenEoX. OpenEoX is an international OASIS Open standard that provides a lightweight, machine-readable (JSON) framework for sharing end-of-life (EOL) and end-of-support (EOS) information for software and hardware products. By integrating seamlessly with tools like SBOMs and the Common Security Advisory Framework (CSAF), OpenEoX enables automated, transparent, and efficient product lifecycle tracking. This integration enables organizations to proactively identify product lifecycle data and unsupported edge devices, streamline vulnerability management, and reduce exposure to security risks. With broad support from industry leaders and government partners—including Cisco, Dell, IBM, Microsoft, Oracle, Red Hat, CISA and BSI—OpenEoX strengthens national defense by enabling timely upgrades and reducing opportunities for exploitation by nation-state actors.

Resources

EXECUTIVE SUMMARY

- Cyentia Institute: Information Risk Insights Study Ransomware
- National Institute of Standards and Technology (NIST): Cybersecurity Framework
- CISA: Secure by Design
- CISA: Cross-Sector Cybersecurity Performance Goals (CPGs)

PART 1: UNDERSTANDING THE CAUSES OF CYBER RISKS AND THE IMPORTANCE OF SECURE BY DESIGN

Vulnerability Trends and Root Causes

- CVE Numbering Authority (CNA)
- Common Weakness Enumerations (CWE)
- CVE Program
- CISA: CVE Quality for a Cyber Secure Future
- CISA: Stakeholder-Specific Vulnerability Categorization (SSVC)
- CISA: Known Exploited Vulnerabilities Catalog
- CISA: Secure by Design Alert: Eliminating OS Command Injection Vulnerabilities
- CISA: The Case for Memory Safe Roadmaps
- MITRE: Unforgivable Vulnerabilities (2007)
- MITRE: Stubborn Weaknesses (2023)
- CWE Top 25 Most Dangerous Software Weaknesses
- CISA: Risk and Vulnerability Assessments

Cyber Risk Landscape

- CISA: Cyber Hygiene Services
- CISA: Vulnrichment Program
- MITRE: MITRE ATT&CK®
- CVE-2025-33073
- CVE-2026-24061
- MITRE: OS Credential Dumping
- CISA: Reported Supply Chain Compromise Affecting XZ Utils Data Compression Library, CVE-2024-3094
- The White House: America's AI Action Plan
- National Security Agency: Deploying AI Systems Securely
- CISA: Safe Software Deployment: How Software Manufacturers Can Ensure Reliability for Customers
- CISA: Secure by Design Alerts
- CISA: Secure Cloud Business Applications (SCuBA) Project
- CISA: Joint Cybersecurity Advisory: Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System

Owning Syber Risk: Secure by Design

- CISA: Safe Software Deployment: How Software Manufacturers Can Ensure Reliability for Customers
- CISA: Product Security Bad Practices
- CISA: Exploring Memory Safety in Critical Open Source Projects
- CISA: Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem
- CISA: The Case for Memory Safe Roadmaps
- CISA: 2026 Minimum Elements for a Software Bill of Materials (SBOM)
- National Telecommunications and Information Administration: 2021 Minimum Elements for a Software Bill of Materials (SBOM)

PART 2: HOW TO IMPROVE YOUR ORGANIZATION'S CYBERSECURITY

Recommendations

- CISA: Cross-Sector Cybersecurity Performance Goals
- NIST: Cybersecurity Framework

CISA's Cyber Risk Reduction Activities and Resources

- CISA: CISA Regions
- CISA: Cross-Sector Cybersecurity Performance Goals
- CISA: Cybersecurity Alerts and Advisories
- CISA: No-Cost Cybersecurity Services and Tools
- CISA: Risk and Vulnerability Assessments
- CISA: Subscribe to Updates from CISA
- OASIS: OpenEoX
- CISA: Binding Operational Directive (BOD) 26-02
- OASIS: Common Security Advisory Framework (CSAF)
- CISA: Coordinated Vulnerability Disclosure Program

Abbreviations

BOD: Binding Operational Directive

CI/CD: Continuous Integration / Continuous Delivery

CNA: CVE Numbering Authority

CPE: Common Platform Enumeration

CPG: Cybersecurity Performance Goals

CSF: Cybersecurity Framework

CVE: Common Vulnerabilities and Exposures

CVSS: Common Vulnerability Scoring System

CWE: Common Weakness Enumeration

CyHy: Cyber Hygiene

DHS: Department of Homeland Security

EOL: End-of-life

EOS: End-of-support

FCEB: Federal Civilian Executive Branch

FTP: File Transfer Protocol

KEV: Known Exploited Vulnerabilities

MFA: Multifactor Authentication

NIST: National Institute of Standards and Technology

PRNI: Pre-Ransomware Notification Initiative

RDP: Remote Desktop Protocol

SBOM: Software Bill of Materials

SCRM: Supply Chain Risk Management

SCuBA: Secure Cloud Business Applications

SMB: Server Message Block

SQL: Structured Query Language

SSL: Secure Sockets Layer

SSVC: Stakeholder-Specific Vulnerability Categorization

TLS: Transport Layer Security

TTPs: Tactics, Techniques, and Procedures

VS: Vulnerability Scanning