CSAI Foundation

Cloud Security Alliance AI Safety Initiative

NVD Enrichment Triage: Enterprise Vulnerability Programs Must Adapt

Unofficial AI-assisted Research

2026-04-19

Key Takeaways

- On April 15, 2026, NIST formally transitioned the National Vulnerability Database to a risk-based triage model, driven by a 263% surge in CVE submissions between 2020 and 2025 [1].
- Approximately 29,000 backlogged CVEs have been reclassified as "Not Scheduled," and going forward only CVEs in the CISA Known Exploited Vulnerabilities catalog, federal government software, and EO 14028 critical software categories will receive full NVD enrichment — an estimated 15–20% of anticipated CVE volume based on the scope of those three categories [2][3].
- The remaining ~80% of CVEs will lack the CPE identifiers, CVSS scores, and CWE classifications that vulnerability scanners and compliance tools rely on to surface and prioritize findings — creating coverage gaps in enterprise security programs whose tooling depends on NVD enrichment.
- Organizations governed by FedRAMP face the most direct compliance exposure, as the program's vulnerability scanning requirements reference NVD-sourced severity scores for remediation timelines [4].
- Enterprises should treat auditing their vulnerability management tooling for NVD dependency as an immediate priority; those that do not may face measurable false-negative rates in scanner output, the extent of which will depend on their software inventory and their scanner platform's enrichment behavior.

Background

The National Vulnerability Database has served as the authoritative enrichment layer for the CVE system since NIST launched it in 2005. While the CVE program assigns identifiers and records basic descriptions, NVD has provided the context — Common Platform Enumeration (CPE) strings for asset matching, Common Vulnerability Scoring System (CVSS) severity scores for prioritization, and Common Weakness Enumeration (CWE) mappings for root-cause tracking — that transforms raw CVE records into operationally useful data. Every major vulnerability scanner, patch management platform, and compliance reporting tool in the enterprise security market was architected around the assumption of NVD enrichment as a universal, timely service.

That assumption no longer holds. CVE submissions climbed 263% between 2020 and 2025, reaching approximately 48,185 disclosures in 2025 alone [1][2]. NIST increased its enrichment output significantly: the agency enriched nearly 42,000 CVEs in 2025, a 45% increase over its previous record [1]. That production gain proved insufficient against the accelerating submission rate. During the first three months of 2026, new CVE submissions ran approximately one-third above the same period in 2025 [1]. Industry analysts are projecting between 50,000 and 70,135 new CVEs by the end of 2026, with a midpoint estimate of 60,000 [5][6]. NIST's own enrichment capacity, even at record output, appears unlikely to close that gap through manual analysis alone without structural changes to the enrichment pipeline.

The consequences accumulated visibly throughout 2024 and into 2025 as a growing backlog of CVEs sat in "Awaiting Analysis" status, lacking the CPE, CVSS, and CWE metadata that downstream tools require. NIST acknowledged the structural problem publicly and committed to finding a sustainable path forward. The April 2026 announcement represents the outcome of that review: rather than attempting universal coverage, NIST will now concentrate enrichment resources on the subset of CVEs most likely to require immediate federal response, while acknowledging that the broader vulnerability landscape will no longer receive systematic enrichment from the agency [1][7].

Security Analysis

The Operational Meaning of Unenriched CVEs

To appreciate the practical impact of the policy change, it is worth being specific about what NVD enrichment provides and what its absence means for operational security tools. A CVE without CPE data is, from the perspective of most vulnerability scanners, effectively invisible. These tools typically match software inventory against NVD-derived CPE strings to generate alerts; where that mapping is absent, affected components may produce no alert in platforms that rely exclusively on NVD enrichment — a risk that grows as the fraction of unenriched CVEs increases. Vendors including Tenable, Qualys, Rapid7, and Wiz maintain independent enrichment pipelines and vendor-advisory feeds that can surface vulnerabilities independently of NVD CPE, and actively exploited vulnerabilities with KEV entries frequently generate alerts through threat-intelligence integrations. Organizations should audit which of these supplemental channels their platforms use before assuming full coverage. VulnCheck, whose commercial NVD++ product competes in the enrichment space, found in its own analysis of 2024 CVE data that NVD provided CPE identifiers for only 41.35% of published vulnerabilities, while VulnCheck's

own enrichment service covered 76.95% of the same population [8]. The April 2026 triage decision will accelerate this divergence by directing NIST's CPE generation effort toward an even narrower subset of CVEs.

CVSS scores carry similar weight. Severity scores drive patch prioritization queues, service-level agreements for remediation windows, and risk acceptance decisions recorded in governance systems. When a CVE lacks a NIST-assigned CVSS score, many organizations default to either the score assigned by the CVE Numbering Authority (CNA) that originally disclosed the vulnerability or to a subjective analyst judgment. Neither alternative is straightforward. NIST's practice of independently scoring CVEs served a quality-assurance function beyond its primary enrichment role. VulnCheck's analysis of dual-scored CVEs documented disagreement between NVD and CNA CVSS scores in more than half of cases, with individual divergences potentially large enough to move a vulnerability across severity tiers from Medium to Critical or vice versa [9]. With NIST no longer routinely re-scoring CNA-assigned CVSS, organizations relying on CNA scores for prioritization are accepting a level of scoring variance that may be invisible in their governance documentation.

The scale of the false-negative risk is not hypothetical. Sonatype's 2026 Software Supply Chain Report documented 167,286 instances of exploitable components going entirely unflagged across the organizations it studied [10] — a gap that NVD enrichment failures help explain, and that the April 2026 triage decision is likely to widen. That figure predates the April 2026 announcement; the coverage deficit will grow as more CVEs enter "Not Scheduled" status.

Asymmetric Coverage and the Open Source Blind Spot

The prioritization model NIST has adopted does not affect all software categories equally. CVEs affecting software used by the federal government and software designated as "critical" under Executive Order 14028 will continue to receive enrichment. Large commercial vendors — Microsoft, Google, Adobe, Oracle — operate as CVE Numbering Authorities and produce detailed, well-structured disclosures that tend to meet enrichment criteria or can be processed efficiently. The software most likely to fall outside priority categories is open source infrastructure, smaller commercial products, and emerging technology stacks.

This asymmetry has immediate implications for AI and cloud-native security postures. Most AI infrastructure libraries — PyTorch, Hugging Face Transformers, ONNX Runtime, LangChain, and similar packages — are unlikely to appear in federal procurement catalogs or EO 14028 critical software designations, meaning vulnerabilities affecting them will generally not meet NIST's new enrichment criteria, even as the enterprise attack surface exposed through AI workloads continues to grow. Organizations that have integrated AI components into production infrastructure face the prospect of operating with incomplete vulnerability coverage for a significant portion of their software inventory —

where CVEs exist but lack the CVSS scores and CPE data needed for automated triage — precisely in software categories that have undergone less security scrutiny and whose vulnerability histories are still being established.

Cloud-native tooling presents a parallel concern. Container runtime vulnerabilities, Kubernetes components, and cloud-provider SDKs may occasionally appear in federal software categories, but comprehensive coverage across the ecosystem is not assured. Security teams relying exclusively on NVD-sourced scanner output should expect coverage gaps in the same software layers that are disproportionately common in modern cloud architectures.

Compliance Exposure Across Regulatory Frameworks

The compliance consequences of the triage shift are most acute for organizations within the FedRAMP authorization boundary. FedRAMP's vulnerability scanning requirements reference NVD-sourced severity scores as the basis for remediation timelines: Critical and High findings carry mandatory remediation windows, and those classifications depend on CVSS scores flowing from NVD [4]. Organizations should consult current FedRAMP program office guidance directly for authoritative requirements, as the characterization of NVD dependency in program documentation may evolve in response to this policy change. Where CVEs are not enriched, the compliance machinery either stalls waiting for scores that will not arrive or must be supplemented with data from sources that FedRAMP documentation does not yet explicitly authorize. Federal agencies and cloud service providers undergoing FedRAMP authorization or continuous monitoring should expect to need formal deviation documentation or updated authorization guidance from FedRAMP's program management office.

Beyond FedRAMP, the impact is more diffuse but real. SOC 2 Type II audits examining vulnerability management processes typically evaluate whether organizations have a consistent, documented methodology for assessing severity and determining remediation priority. NVD-derived CVSS scores have served as the standard evidence artifact for that evaluation. Auditors confronting an environment where a meaningful fraction of CVEs lack CVSS scores will need guidance from organizations on how alternative severity determinations were made and documented. Absent that narrative, audit findings related to incomplete vulnerability tracking are a foreseeable outcome. Similar considerations apply to ISO 27001 certifications, DORA compliance programs that reference severity-tiered remediation obligations, and HIPAA covered entities that have codified NVD-based risk assessments into their vulnerability management policies.

The broader governance issue is that enterprise risk dashboards, board-level security reporting, and executive risk acceptance frameworks are often calibrated to CVSS thresholds. A vulnerability program that silently stops surfacing a large fraction of CVEs does not become more secure — it becomes less

visible. Organizations that do not actively compensate for the enrichment gap will find their risk posture understated in ways that may not surface until an incident occurs.

Recommendations

Immediate Actions

Security teams should treat this as an immediate priority: auditing the data sources their vulnerability management platforms use to retrieve CVSS scores, CPE data, and CWE classifications. Most enterprise scanners offer configuration options specifying which enrichment feeds they consume; identifying those settings and mapping them to NVD dependency is a prerequisite for understanding exposure. Teams using platforms that rely exclusively on NVD should open a vendor inquiry asking what the vendor's plan is for CVEs that NIST designates as "Not Scheduled" — whether the vendor will supplement from alternative sources and on what timeline.

Organizations operating under FedRAMP authorization should initiate contact with their Authorizing Official and the FedRAMP Program Management Office to document the change in NVD coverage and request guidance on acceptable alternative data sources for CVEs that lack NVD enrichment. Proceeding without that documentation exposes continuous-monitoring attestations to technical findings.

Short-Term Mitigations

A high-value interim mitigation is integrating the CISA Known Exploited Vulnerabilities catalog as the primary signal for exploitation urgency. CISA's KEV catalog aggregates evidence of active exploitation and now forms the backbone of NIST's own enrichment priority queue; treating KEV entries as the highest-urgency tier of the remediation pipeline is both directionally sound and aligned with NIST's expressed priorities [11]. This approach also carries no licensing cost, relies on a .gov authoritative source, and can be implemented through most enterprise scanner platforms without custom integration. EPSS (Exploit Prediction Scoring System) scores provide complementary exploitation-likelihood estimates for CVEs not yet in KEV and should be incorporated into prioritization workflows alongside CVSS wherever available [12].

To close the CPE and CVSS gap for CVEs that NIST will not enrich, organizations should evaluate supplemental enrichment sources including VulnCheck NVD++ [8], the GitHub Advisory Database, OSV.dev, and commercial threat intelligence platforms that maintain independent enrichment pipelines.

These feeds vary in coverage, timeliness, and licensing terms, but collectively they offer a materially better signal than an unenriched CVE record. Organizations should not treat any single alternative source as a full replacement for NVD; a tiered approach that combines KEV, EPSS, CNA-provided CVSS with documented score-confidence caveats, and commercial enrichment feeds will produce more reliable prioritization than any single substitute.

Vulnerability management policy documentation should be updated to acknowledge the changed NVD enrichment model and specify the organization's chosen alternative data sources, quality-assurance methodology for CNA-assigned CVSS scores, and escalation path for CVEs where enrichment data is absent or conflicting. This documentation update is not optional for organizations subject to audit; it is the evidence artifact that demonstrates the vulnerability program's continued fitness for purpose under changed external conditions.

Strategic Considerations

The April 2026 announcement reflects a structural mismatch between CVE submission volume and any single organization's enrichment capacity — NIST's or otherwise. The long-term response from the security community will likely involve some combination of automated enrichment pipelines, expansion of CNA program participation, and federated community enrichment efforts. Security leaders should monitor these developments and consider contributing organizational expertise or resources, given that the quality of community-produced enrichment data will directly affect the reliability of commercial tooling that consumes it.

Enterprises with large open source footprints — and particularly those with significant AI infrastructure dependencies — should consider whether direct engagement with the maintainers and CNA programs of their highest-risk dependencies is warranted. Where a software project does not currently operate as a CNA, its CVEs may arrive in the NVD with minimal metadata and no prospect of NIST enrichment. Direct advisory relationships with key upstream maintainers, or participation in programs like the GitHub Advisory Database, can provide earlier and more complete vulnerability intelligence than waiting for NVD records.

Finally, organizations should initiate a review of how vendor contracts for vulnerability management tooling address the NVD dependency question. If a scanner's SLA for CVE detection is implicitly predicated on NVD enrichment, and the vendor does not commit to supplemental coverage, that contract may no longer reflect the service level organizations are actually receiving. Procurement and renewal discussions should include explicit questions about enrichment data sources and coverage commitment for CVEs outside NIST's priority categories.

CSA Resource Alignment

The NVD enrichment shift intersects with multiple areas of CSA's published guidance and ongoing program work.

CSA AI Controls Matrix (AICM) is particularly relevant here because AI infrastructure libraries and ML frameworks represent a disproportionate share of the software ecosystem that will fall outside NIST's enrichment priority categories. Organizations implementing AICM to govern their AI system security posture should treat CVE coverage for AI software dependencies as an explicit control gap that requires compensating measures. The AICM's supply chain security controls provide the governance scaffolding for documenting these compensating measures and tracking their effectiveness.

CCM v4.1 — Threat and Vulnerability Management domain addresses the processes by which organizations maintain awareness of vulnerabilities in their environments and prioritize remediation. The CCM's framework for risk-based TVM aligns with the direction NIST itself is moving: not every vulnerability demands equal urgency, and programs built on contextual risk assessment rather than universal CVSS-threshold automation are better positioned to absorb changes in enrichment completeness. CCM v4.1 implementers should review their TVM controls documentation to ensure they specify data sources and quality assurance processes rather than implicitly assuming NVD universal coverage.

CSA STAR Program continuous monitoring attestations that reference NVD-sourced CVSS scores as compliance evidence will require updating to reflect the changed enrichment landscape. Organizations pursuing STAR Level 2 or Level 3 certifications should work with their assessors to establish what constitutes acceptable alternative evidence for vulnerability severity classification in the post-NVD-triage environment.

MAESTRO (Agentic AI Threat Modeling) is relevant because agentic systems operating in enterprise environments are themselves consumers of vulnerability intelligence, often as inputs to automated remediation workflows or security posture reporting. Where an agent's decision logic depends on NVD-enriched CVE data, the enrichment gap introduces a risk surface that should be documented as part of the agent's threat model.

AI Organizational Responsibilities: Core Security Responsibilities (CSA, 2024) outlines the security obligations organizations take on when deploying AI systems, including responsibility for the software supply chain of AI components. The NVD enrichment gap makes fulfilling those responsibilities harder through conventional tooling and strengthens the case for the kind of direct engagement with AI software maintainers discussed in the strategic recommendations above.

References

[1] NIST. "NIST Updates NVD Operations to Address Record CVE Growth." NIST News, April 2026.

[2] Toulas, Bill. "NIST Limits CVE Enrichment After 263% Surge in Vulnerability Submissions." The Hacker News, April 2026.

[3] Kovacs, Eduard. "NIST Drops NVD Enrichment for Pre-March 2026 Vulnerabilities." Infosecurity Magazine, April 2026.

[4] Geller, Eric. "NIST limits vulnerability analysis as CVE backlog swells." Cybersecurity Dive, April 2026.

[5] Gooding, Sarah. "NIST Officially Stops Enriching Most CVEs as Vulnerability Volume Soars." Socket.dev Blog, April 2026.

[6] Shah, Sooraj. "Reliable CVE sources in the age of NIST NVD cutbacks." Aikido Security Blog, April 2026.

[7] Kapko, Matt. "NIST narrows scope of CVE analysis to keep up with rising tide of vulnerabilities." CyberScoop, April 2026.

[8] VulnCheck. "Outpacing NIST NVD with VulnCheck NVD++." VulnCheck Blog, 2024.

[9] VulnCheck. "Who to Trust? National Vulnerability Database CVSS Accuracy Issues." VulnCheck Blog (date unknown).

[10] Sonatype. "Vulnerability Management – 2026 Software Supply Chain Report." Sonatype, 2026.

[11] CISA. "Known Exploited Vulnerabilities Catalog." CISA, continuously updated.

[12] FIRST. "Exploit Prediction Scoring System (EPSS)." Forum of Incident Response and Security Teams, continuously updated.

Further Reading

- Flashpoint. "National Vulnerability Database Shifts to Selective Enrichment as CVE Volume Surges." Flashpoint Blog, April 2026.

- Endor Labs. "Surge in submissions forces NIST to change how it handles CVEs." Endor Labs Blog, April 2026.
- Help Net Security. "NIST admits defeat on NVD backlog, will enrich only highest-risk CVEs going forward." Help Net Security, April 16, 2026.
- SiliconANGLE. "NIST shifts National Vulnerability Database to risk-based triage as CVE submissions hit record levels." SiliconANGLE, April 15, 2026.