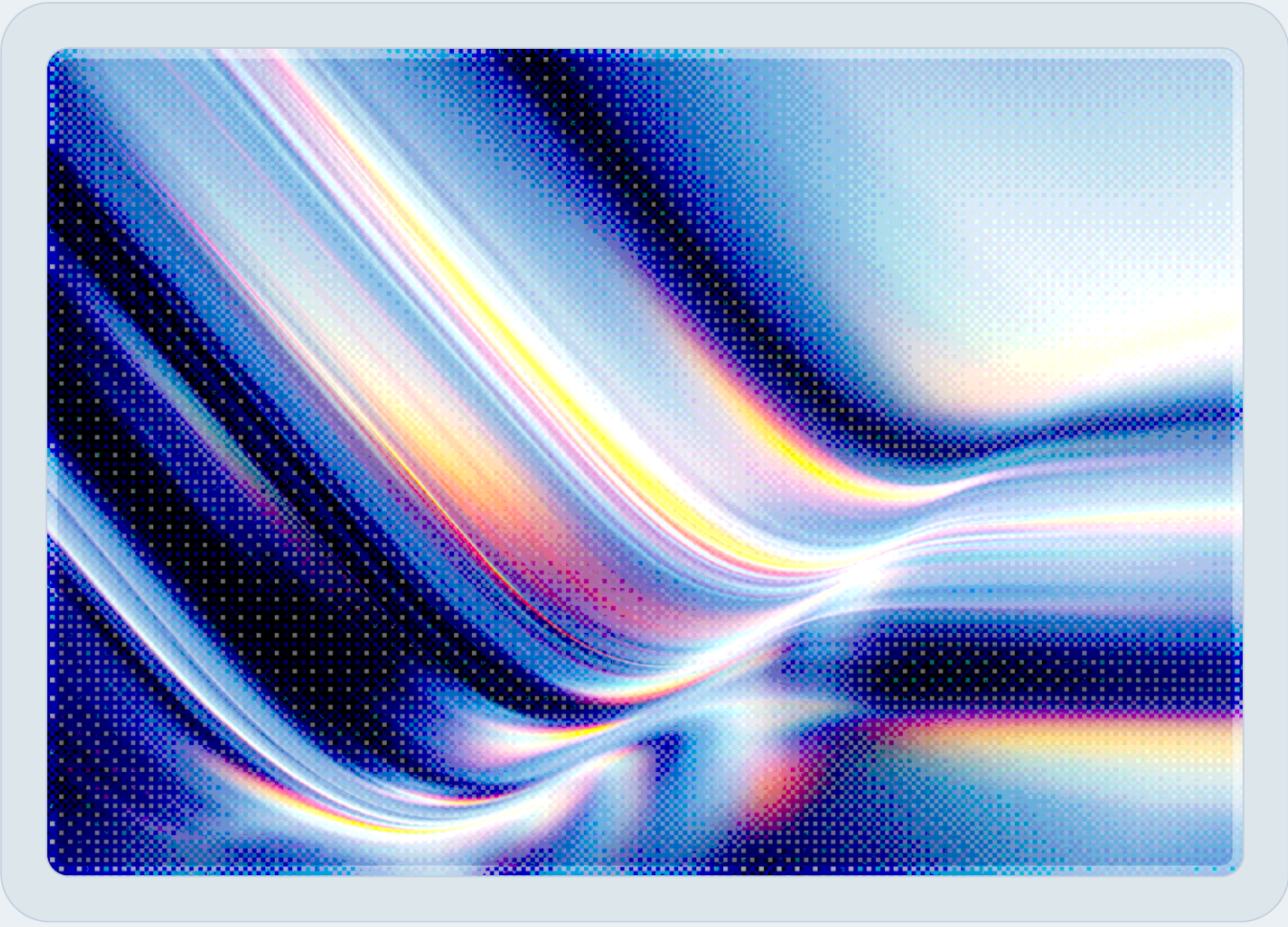
CSAI Foundation | Cloud Security Alliance

NVD Triage Overhaul: End of Universal CVE Enrichment

How NIST's Risk-Based Model Disrupts Enterprise Vulnerability Programs

2026-04-29

AI-assisted Rapid Research



CSAI

cloud security alliance®

Key Takeaways

On April 15, 2026, NIST formally abandoned its longstanding goal of fully analyzing every CVE submitted to the National Vulnerability Database (NVD), transitioning to a risk-based triage model that reserves complete metadata enrichment for a narrow subset of vulnerabilities [1][2]. The change was driven by a 263% surge in CVE submissions between 2020 and 2025 – a volume that outpaced NIST's capacity even after the program enriched nearly 42,000 CVEs in 2025, a 45% improvement over any prior year [1][3]. Going forward, only CVEs appearing in CISA's Known Exploited Vulnerabilities (KEV) catalog, CVEs affecting software used within the federal government, and CVEs for critical software as defined by Executive Order 14028 will receive full NIST enrichment – an estimated 15–20% of projected annual CVE volume [1][4].

The remaining approximately 80% of CVEs will be catalogued in the NVD without the CPE identifiers, CVSS severity scores, and CWE weakness classifications that vulnerability scanners, patch management platforms, and compliance reporting tools rely upon to surface and prioritize findings [1][5]. Approximately 29,000 backlogged CVEs with an NVD publish date earlier than March 1, 2026 have already been reclassified to "Not Scheduled" status, meaning they will receive no enrichment unless explicitly requested [1][6]. Because most enterprise vulnerability scanners map CVEs to affected products through CPE identifiers, a CVE that lacks CPE data is operationally invisible to automated detection pipelines – organizations that do not supplement NVD with alternative intelligence sources will face growing blind spots in their vulnerability programs.

Background

The National Vulnerability Database has functioned as the authoritative backbone of commercial vulnerability management since its establishment in 2005. By providing standardized enrichment metadata – Common Platform Enumeration (CPE) identifiers that map vulnerabilities to specific software products and versions, Common Vulnerability Scoring System (CVSS) severity scores, and Common Weakness Enumeration (CWE) root-cause classifications – NVD created a universal language that every scanner, compliance framework, and security operations tool in the industry learned to speak [7]. For two decades, enterprise security programs were architected around the assumption that this enrichment would be timely and universal, and regulatory frameworks, vendor contracts, and internal policies all adopted NVD-sourced data as a de facto standard.

That assumption began to fracture in early 2024, when a funding disruption forced NIST to temporarily pause metadata enrichment for incoming CVEs, producing the first significant backlog since the database's founding [8]. NIST contracted with CISA in August 2024 to address the backlog and improve throughput, and enrichment productivity rose substantially through 2025 [1]. But the CVE disclosure ecosystem was simultaneously expanding beyond the reach of manual enrichment pipelines. The number of CVE Numbering Authorities authorized to assign CVE identifiers has grown steadily for several years, and AI-assisted vulnerability research — both from security researchers and from increasingly capable autonomous systems — is generating discoveries at rates that pre-date any scaling plan NIST had in place. Even at its highest recorded enrichment throughput, NIST was falling further behind absolute submission volume [3][9].

The April 2026 policy shift is therefore a formal institutional acknowledgment that universal enrichment is no longer a viable operating model. Rather than continue framing the backlog as a temporary condition to be resolved, NIST has restructured its enrichment mission around explicit prioritization. The policy change carries two additional modifications that deserve attention. First, NIST has revised its re-analysis policy: whereas it previously re-analyzed all modified CVEs after initial enrichment, it will now re-analyze a CVE only if it determines a modification materially affects the enrichment data [1]. Second, NIST has announced it will no longer routinely issue its own CVSS score for CVEs where the submitting CNA has already provided one, deferring to CNA-sourced scoring for that portion of submissions [1][2].

Security Analysis

The Enrichment Gap and Its Operational Consequences

The practical severity of the new triage policy is almost entirely determined by how tightly an organization's vulnerability management infrastructure is coupled to NVD-sourced metadata. Every major commercial scanner — Tenable Nessus, Qualys VMDR, Rapid7 InsightVM, Wiz, and their contemporaries — was designed during an era when NVD CPE data was assumed to be comprehensive and timely. Scan result correlation, software bill of materials (SBOM) analysis, and automated patch prioritization workflows are commonly built on CPE-to-product matching logic. A CVE that lacks CPE data still exists in NVD as a record, but it becomes operationally invisible to tooling that depends on that matching logic to surface findings against a specific product inventory [1][5][10]. The consequence is silent blind spots: a scanner finishes its sweep, reports no findings for an affected product, and neither the scanner nor the analyst has any signal that a relevant vulnerability was missed.

CVSS score gaps present a parallel problem. Compliance frameworks, service-level agreements, and internal vulnerability management policies almost universally reference CVSS thresholds as the basis for prioritization and remediation timelines. A CVE that lacks a NIST-issued CVSS score cannot be automatically placed in the remediation queue that those policies describe. NIST has announced that CNA-supplied CVSS scores will now surface in NVD records, partially filling this gap — but CNA coverage is inconsistent across vendors and product categories, and CNA-supplied scores have historically received less external scrutiny than NIST-validated ones. The result is a heterogeneous scoring landscape in which some CVEs carry scores from multiple sources that may disagree, while others have no score at all.

The 29,000 backlogged CVEs reclassified to "Not Scheduled" represent a discrete near-term risk that differs from the ongoing gap. These are vulnerabilities disclosed before March 1, 2026 that exist in the public record — catalogued by researchers, discussed in security advisories, and potentially known to threat actors — but that may lack the structured CPE and CVSS metadata that automated tooling would need to detect and prioritize them. VulnCheck research published in 2025 found that a meaningful portion of CVEs in the NVD backlog at that time had associated exploitation activity [12], and the reclassification of this cohort to "Not Scheduled" means that any exploitation-linked CVE without its own CISA KEV listing will remain enrichment-deprived unless a specific enrichment request is submitted to NIST at nvd@nist.gov.

Regulatory and Compliance Exposure

The enrichment policy change creates downstream compliance exposure that most organizations have not yet fully mapped. FedRAMP's continuous monitoring requirements reference NVD-sourced severity scores as a basis for prioritizing remediation timelines. Agencies and contractors operating under FedRAMP authorization whose vulnerability management plans rely on NVD CVSS scores may find those plans functionally impaired for the 80% of CVEs that will not receive enrichment. The FedRAMP Program Management Office had not issued formal guidance on alternative data sources as of this writing, creating an interim compliance ambiguity that organizations should proactively address by documenting the policy change and seeking AO guidance rather than waiting for program-level clarification.

For organizations governed by ISO/IEC 27001, DORA, or HIPAA, the exposure is comparable if less acute. Where vulnerability management policies reference NIST or NVD severity classifications by name — a common pattern adopted during the NVD's era of comprehensive coverage — those policies now describe a data source that no longer provides the coverage they assumed. Updating policies and tool configurations to accommodate alternative enrichment sources may require coordination across security, legal, and compliance functions and may trigger control assessments depending on certification scope.

Organizations subject to DORA's vulnerability management obligations should confirm with their competent authority whether CNA-supplied CVSS scores or alternative commercial enrichment sources are acceptable substitutes, rather than assuming equivalence.

AI-Accelerated Disclosure and Structural Pressure

The CVE volume crisis driving the April 2026 policy change is itself a symptom of a structural shift in how vulnerabilities are discovered. Advanced AI systems are increasingly capable of autonomous code analysis at a scale and speed that human researchers cannot match, and the practical consequence is a sustained increase in disclosure rates that will persist independent of NVD's enrichment throughput. The CVE ecosystem — and the NVD in particular — was designed around human-paced discovery rhythms, and the combination of expanding CNA membership and AI-assisted research suggests that annual submission volumes will continue to grow well beyond the 263% increase already recorded between 2020 and 2025 [3][9]. The April 2026 triage policy is therefore better understood as a floor than a ceiling: without sustained changes to how the broader ecosystem funds and structures vulnerability enrichment, the coverage gap will widen over time.

This structural dynamic has a direct implication for enterprise planning. Organizations that treat the current enrichment gap as a temporary deviation — something to route around until NVD recovers — are miscalibrating the risk. The gap is structural, not episodic. Programs that adapt by formally diversifying their vulnerability intelligence architecture will be more resilient to the continued evolution of both CVE submission volumes and NIST's enrichment capacity.

Alternative Intelligence Sources

The security industry's response to the 2024 NVD backlog accelerated development of independent enrichment pipelines that now provide meaningful supplemental coverage. VulnCheck NVD++ reported CPE coverage for 76.95% of CVEs published in 2024, compared to 41.35% for NIST NVD at that time, with CPE data delivered an average of four days faster [13]. VulnCheck exposes this data through an API compatible with the NVD 2.0 format, making integration with existing tooling operationally straightforward. The GitHub Advisory Database provides ecosystem-native vulnerability data for packages across npm, PyPI, Go, Maven, RubyGems, and other registries, with particular depth for open-source components that NVD's CPE model covers inconsistently [14]. Google's OSV aggregates vulnerability data across multiple upstream sources with package-ecosystem granularity and an open API, offering an open alternative to commercial enrichment vendors.

EPSS — the Exploit Prediction Scoring System, maintained by FIRST — addresses the prioritization problem from a different angle by using machine learning to estimate the probability that a given CVE will be actively exploited within a 30-day window [15]. EPSS scores update dynamically as threat intelligence evolves, making them a complement rather than a replacement for static CVSS scores. Organizations that have incorporated EPSS alongside CVSS in their prioritization logic already have a richer signal for triage decisions and will be better positioned to compensate for the gaps introduced by the new NVD policy. The CISA KEV catalog itself should also be treated as a primary intelligence feed rather than a secondary one — because NIST commits to enriching KEV-listed CVEs within one business day, the KEV catalog now represents the highest-confidence intersection of NVD enrichment and real-world exploitation evidence available in the new environment [1][4][7].

Recommendations

Immediate Actions

Security operations and vulnerability management teams should audit their scanner and SIEM integrations to identify which tools pull CVSS scores, CPE identifiers, or CWE classifications directly from NVD API endpoints. Where a direct dependency exists, teams should contact the vendor to confirm whether independent enrichment pipelines are active and how the tool behaves when a CVE lacks NVD enrichment. Tenable, among others, has published guidance indicating it maintains supplemental enrichment feeds [16]; teams should verify those feeds are enabled and review the vendor's handling of enrichment gaps before assuming existing scan coverage is unaffected.

Organizations with FedRAMP authorizations should document the NVD policy change and proactively engage their Authorizing Official to assess whether their continuous monitoring plan requires amendment. NIST has confirmed that enrichment requests for specific high-priority CVEs can be submitted to nvd@nist.gov [1]; teams should establish a workflow for submitting such requests when a CVE affecting their environment lacks enrichment and falls outside the three prioritized categories.

Short-Term Mitigations

Within 30 to 60 days, organizations should formalize the CISA KEV catalog as a primary — not optional — input to their vulnerability prioritization workflow. Because NIST commits to enriching KEV-listed CVEs within one business day, the KEV catalog now anchors the highest-confidence, most timely subset of

NVD enrichment. Every CVE on the KEV catalog carries both structured NVD metadata and documented active exploitation evidence, making it the unambiguous first-priority signal in the new environment [1][4][7].

Teams should evaluate supplemental enrichment sources — VulnCheck NVD++, the GitHub Advisory Database, OSV, and EPSS — based on their technology stack composition and risk profile. Organizations with substantial open-source software exposure will find that ecosystem-native databases provide meaningfully better coverage for their specific risk surface than a single NVD-centric alternative. Vendor security advisory feeds should be systematically incorporated into vulnerability management workflows, as they represent direct, authoritative enrichment for a vendor's own products that NVD's pipeline only partially replicated.

Vulnerability management policies that reference NIST CVSS scores by name should be reviewed to confirm whether CNA-supplied CVSS scores from the NVD record — or scores sourced from vendor advisories — are acceptable substitutes under the policy language, and amended if not. This review is operationally scoped and can typically be completed without triggering a formal audit cycle.

Strategic Considerations

The NVD triage policy accelerates an already-visible shift in vulnerability management practice away from single-database prioritization and toward multi-source intelligence integration. Organizations that have invested in threat intelligence platforms capable of aggregating CISA KEV, EPSS, vendor advisories, ISAC feeds, and commercial enrichment will find this transition less disruptive than those whose programs are tightly coupled to a single authoritative data source. Security leaders should treat the current disruption as the impetus for a formal architecture review — documenting every intelligence source the vulnerability program consumes, the confidence level assigned to each, and the procedures for handling gaps in any single source.

SBOM adoption also becomes more strategically important in this environment. A software bill of materials allows an organization to map its component inventory against vulnerability databases using package-level identifiers rather than CPE-based product matching, providing a detection mechanism for vulnerabilities that may lack NVD CPE enrichment entirely. Investment in SBOM generation and analysis tooling reduces the detection dependency on NVD's enrichment pipeline, though it does not eliminate the need for severity and exploitation-likelihood data at the prioritization layer. Longer term, organizations should advocate within their industry associations and standards bodies for a more sustainable model of vulnerability enrichment — whether through expanded public funding, industry consortium maintenance of enrichment data, or formalized CNA responsibilities for enrichment quality — to address the structural insufficiency that the April 2026 policy change reflects.

CSA Resource Alignment

CSA's own research anticipated several dimensions of the current crisis. The CSA Vulnerability Data Working Group report "Top Concerns with Vulnerability Data" (2024) examined the growing insufficiency of CVE and CVSS frameworks for managing modern IT threat intelligence requirements, identifying outdated data, limited contextual coverage, and scoring inconsistencies as systemic problems requiring structural remediation [17]. The April 2026 NVD triage policy is, in effect, an official acknowledgment that the resource constraints underlying those systemic problems have now become unmanageable within the current enrichment model.

CSA's April 2026 "AI Vulnerability Storm" briefing frames AI-accelerated vulnerability discovery as a structural shift in offensive capability that creates an accelerating backlog of both new disclosures and remediations. The same AI-driven productivity improvements that are expanding the pool of discovered vulnerabilities are also the proximate cause of the submission volume increase that forced the NVD triage overhaul. Organizations building AI-resilient security programs must account for the enrichment gap as a permanent condition of their operating environment, not an exceptional disruption.

The Cloud Controls Matrix (CCM) v4.0 contains controls in the Threat and Vulnerability Management (TVM) domain that address vulnerability scanning, risk rating, and remediation timelines. Organizations that have codified CCM TVM controls into compliance programs should review whether those controls implicitly reference NVD-specific data requirements and update implementation guidance to reflect the broader multi-source intelligence architecture described above. CSA's AI Controls Matrix (AICM) is additionally relevant for organizations deploying AI-assisted security tooling that itself queries NVD APIs: the AICM's guidance on data quality assurance and control validation for AI-integrated workflows provides a governance framework for ensuring that enrichment gaps do not propagate undetected through AI-mediated vulnerability management pipelines.

Finally, CSA's STAR program — which assesses cloud provider security posture against CCM controls — provides a mechanism for enterprises to evaluate whether their cloud service providers' vulnerability management programs are accounting for the NVD enrichment change. Procurement and vendor risk teams should consider adding questions about NVD supplemental enrichment sources to STAR assessments and vendor security questionnaires.

References

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

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

[3] SiliconANGLE. "NIST shifts National Vulnerability Database to risk-based triage as CVE submissions hit record levels." SiliconANGLE, April 15, 2026.

[4] SecurityWeek. "NIST Prioritizes NVD Enrichment for CVEs in CISA KEV, Critical Software." SecurityWeek, April 2026.

[5] Security Boulevard. "NVD Changes 2026: Why public vulnerability data is no longer enough." Security Boulevard, April 2026.

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

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

[8] IBM Security. "CVE backlog update: The NVD struggles as attackers change tactics." IBM, 2025.

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

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

[11] Security Magazine. "NIST's New Prioritization Criteria for CVEs, Examined by Experts." Security Magazine, April 2026.

[12] VulnCheck. "Danger is Still Lurking in the NVD Backlog." VulnCheck Blog, 2025.

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

[14] GitHub. "GitHub Advisory Database." GitHub, continuously updated.

[15] FIRST. "Exploit Prediction Scoring System (EPSS)." FIRST, continuously updated.

[16] Tenable. "As the NVD scales back CVE enrichment, here's what Tenable customers need to know." Tenable Blog, April 2026.

[17] Cloud Security Alliance. "Top Concerns with Vulnerability Data." CSA Vulnerability Data Working Group, 2024.