INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-17 14:05 UTC

NIST NVD Triage Shift Creates Structural Gap in Vulnerability Intelligence for Non-KEV CVEs

GOVERNANCE | HIGH | CVSS 7.5

SCC Item ID	SCC-GOV-2026-0016
Type	Governance
Severity	HIGH
CVSS Base Score	7.5
Affected Products	All organizations relying on NVD as primary vulnerability enrichment source; NIST National Vulnerability Database (NVD); CISA Known Exploited Vulnerabilities (KEV) catalog
Published	2026-04-17T03:14:00
Discovery Source	Rss

Executive Summary

Effective April 15, 2026, NIST formally restricted NVD enrichment to CVEs in CISA's KEV catalog, federal agency software, and EO 14028-designated critical software, leaving the majority of newly published CVEs without CVSS scores, CWE classifications, or CPE data. Any organization using NVD as its primary or sole vulnerability enrichment source now faces gaps in automated risk scoring and patch prioritization. Without immediate action to supplement NVD with alternative enrichment sources, security teams will triage against incomplete intelligence, raising the likelihood of unaddressed exposure.

Technical Analysis

NIST's April 15, 2026 operational change restricts automatic enrichment, CVSS scoring, CWE mapping, CPE enumeration, to three categories: (1) CVEs listed in CISA KEV, (2) software used by U.S. federal agencies, and (3) software meeting EO 14028 critical software definitions. All CVEs outside these categories are now assigned 'Not Scheduled' enrichment status. NIST reports a 263% increase in CVE submissions between 2020 and 2025, with Q1 2026 volume running 33% above Q1 2025 as rationale for the policy change. The structural consequence is that vulnerability scanners, SIEM enrichment pipelines, SOAR playbooks, and risk scoring models that pull CVSS base scores, CWE classifications, or CPE strings from NVD APIs will now receive null or incomplete records for the majority of newly published CVEs. This degrades automated severity banding, asset matching, and patch prioritization logic. CWE-693 (Protection Mechanism Failure) and CWE-1035 (Using Components with Known Vulnerabilities; OWASP Top Ten 2021 A06) are relevant as secondary risk descriptors for organizations now operating with reduced visibility into component-level exposure. MITRE techniques T1190 (Exploit Public-Facing Application), T1203 (Exploitation for Client Execution), and T1068 (Exploitation for

Privilege Escalation) represent exploitation classes most likely to benefit from reduced detection friction in environments relying solely on NVD-sourced scoring. In such environments, unenriched CVEs may face reduced internal detection friction, potentially increasing the exploitation window before discovery. Source: NIST (https://www.nist.gov/news-events/news/2026/04/nist-updates-nvd-operations-address-record-cve-growth).

Action Checklist

1. Step 1: Assess Exposure. Audit your vulnerability management pipeline to identify every component that pulls enrichment data from NVD APIs (CVSS scores, CWE, CPE). Document which scanners, SIEM enrichment jobs, SOAR playbooks, and risk scoring tools depend on NVD as a primary or sole source. This scoping step is required before any remediation action is meaningful.
2. Step 2: Identify Gaps. Query your vulnerability management platform for CVEs currently marked 'Not Scheduled' or missing CVSS/CWE/CPE data in NVD as of April 15, 2026. Cross-reference your active asset inventory against these unenriched CVEs to determine your current blind-spot surface. Prioritize CVEs affecting internet-facing or high-value assets.
3. Step 3: Supplement Enrichment Sources. Integrate at least one alternative enrichment source to cover the NVD gap. Evaluated options include OSV.dev (open-source ecosystem coverage), vendor-direct advisories via OVAL or SBOM feeds, and commercial threat intelligence platforms with independent CVSS scoring. Configure pipeline fallback logic to pull from secondary sources when NVD fields return null.
4. Step 4: Validate Pipeline Integrity. After integrating alternative sources, run a validation pass against a known CVE set to confirm enrichment fields are populating correctly across your toolchain. Test CVSS score ingestion, CWE tagging, and CPE asset matching end-to-end. Establish a recurring check, weekly minimum, to detect future enrichment gaps before they compound.
5. Step 5: Update Prioritization Logic and Governance. Revise your vulnerability prioritization policy to explicitly acknowledge NVD's reduced scope. Define a documented fallback hierarchy for enrichment sources. Update SLAs for patch prioritization to account for delayed or absent CVSS data. Communicate the change to vulnerability management, SOC, and GRC teams. Log the policy update for audit trail purposes.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and GRC leadership immediately if audit, assessment, or regulatory review is scheduled within 90 days and the organization cannot demonstrate an alternative enrichment source is operational, or if any post-April-15-2026 unenriched CVE is identified on an internet-facing or PCI/HIPAA-scoped asset without a documented risk acceptance — the absence of CVSS data does not eliminate reporting obligations under those frameworks.
Recovery Notes	Recovery is complete when the vulnerability management pipeline demonstrably produces CVSS scores, CWE tags, and CPE mappings for newly published CVEs from at least one non-NVD source, and the recurring weekly validation check has run cleanly for two consecutive cycles. Monitor enrichment null-field rates weekly for a minimum of 90 days post-integration to catch secondary gaps (e.g., OSV.dev ecosystem coverage gaps for proprietary software, vendor OVAL feed latency). Verify that all downstream consumers — SIEM risk scoring rules, SOAR triage playbooks, and patch prioritization SLAs — are operating against enriched data before closing the incident record.

Forensic Artifacts	NVD API raw JSON responses (timestamped) for CVEs published on or after April 15, 2026 — specifically records where `metrics`, `weaknesses`, and `configurations` arrays are empty, serving as documentary evidence of the enrichment gap scope | Scanner output exports (Nessus `.nessus` exports, OpenVAS XML reports, or Trivy JSON output) filtered to 'CVSS: N/A' or unscored findings generated after April 15, 2026 — these identify which assets and CVEs fell into the blind spot during the gap period | Vulnerability management platform configuration files and SOAR playbook definitions showing hardcoded NVD API dependencies (e.g., `api.nvd.nist.gov` references in enrichment job configs) — evidence of which pipeline components were affected and required remediation | Pre- and post-integration enrichment validation logs (dated CSV or JSON) showing field population rates before and after fallback source integration — demonstrates remediation efficacy and documents residual unenriched CVEs requiring manual triage | Version-controlled policy document diff and stakeholder communication records (email or meeting notes) documenting the governance response to the NVD scope change, including revised SLAs and fallback source hierarchy — required audit trail evidence for compliance reviews referencing the post-April-15-2026 period

Per-Action IR Details

Step 1: Assess Exposure — Audit your vulnerability management pipeline to identify every component that pulls enrichment data from NVD APIs (CVSS scores, CWE, CPE). Document which scanners, SIEM enrichment jobs, SOAR playbooks, and risk scoring tools depend on NVD as a primary or sole source. This scoping step is required before any remediation action is meaningful.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establish and maintain IR capability, including tooling inventory and dependency mapping for detection and analysis pipelines

Controls: NIST IR-4 (Incident Handling) — preparation sub-phase requires documented capability inventory, NIST SI-5 (Security Alerts, Advisories, and Directives) — receiving and acting on advisories about changes to external intelligence sources, NIST RA-3 (Risk Assessment) — assessing risk introduced by loss of enrichment fidelity in the vulnerability management pipeline, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — process documentation must identify all enrichment dependencies, CIS 2.1 (Establish and Maintain a Software Inventory) — scanner and toolchain components consuming NVD APIs must appear in the software inventory

Compensating: Run `grep -r 'nvd.nist.gov\|services.nvd.nist.gov' /etc/` and equivalent config directories for Tenable Nessus (`/opt/nessus/`), OpenVAS (`/etc/openvas/`), and Trivy (`~/.trivy/`) to surface hardcoded NVD API calls. For SOAR/SIEM enrichment jobs, export playbook/rule configs and pipe through `grep -i 'nvd\|nist.*cve\|cvss.*nist'` to enumerate affected automations. Document results in a two-column spreadsheet: tool name | NVD dependency type (CVSS/CWE/CPE/API key).

Evidence: Before remediating, snapshot the current state of your vulnerability management toolchain: export scanner configuration files (e.g., Nessus `.nessus` policy exports, OpenVAS scan configs via `gvm-cli`), capture SOAR playbook definitions referencing NVD enrichment steps, and record current API call logs from NVD (`api.nvd.nist.gov/rest/json/cves/2.0`) showing which tools are authenticating. This baseline documents your pre-gap exposure state for audit trail purposes under NIST IR-5 (Incident Monitoring) and establishes the scope boundary for gap analysis in Step 2.

Step 2: Identify Gaps — Query your vulnerability management platform for CVEs currently marked 'Not Scheduled' or missing CVSS/CWE/CPE data in NVD as of April 15, 2026. Cross-reference your active asset inventory against these unenriched CVEs to determine your current blind-spot surface. Prioritize CVEs affecting internet-facing or high-value assets.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Analyze adverse events (here, the structural gap in enrichment data) to understand scope, impact, and affected assets; correlate incomplete data signals across sources

Controls: NIST SI-4 (System Monitoring) — monitoring must detect when enrichment pipelines are returning null or incomplete fields, which constitutes an adverse signal, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review vulnerability scan outputs for systematic absence of CVSS/CWE/CPE fields introduced by the NVD policy change, NIST RA-3 (Risk Assessment) — unenriched CVEs on internet-facing or high-value assets require immediate risk assessment using available data sources, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — process must include detection of enrichment failures, not just vulnerability presence, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory) — cross-referencing unenriched CVEs against asset inventory requires that inventory to be current and accurate

Compensating: For teams without a commercial VM platform, query the NVD API directly: `curl 'https://services.nvd.nist.gov/rest/json/cves/2.0?pubStartDate=2026-04-15T00:00:00&pubEndDate=2026-04-16T00:00:00' | python3 -m json.tool | grep -c 'cvssMetricV3'` to count CVEs published post-cutoff with no CVSS data. Cross-reference your asset inventory (exported from osquery: `SELECT name, version FROM programs;` on Windows or `SELECT name, version FROM deb_packages;` on Linux) against unenriched CVE product strings manually. Flag any match where the NVD `metrics` array is empty and the asset is internet-facing.

Evidence: Capture NVD API responses for all CVEs published on or after April 15, 2026, and store raw JSON — specifically preserving records where the `metrics`, `weaknesses`, and `configurations` arrays are empty or absent. These null-field responses are the forensic record of the gap. Additionally, export your scanner's current vulnerability findings list filtered to 'CVSS: N/A' or 'unscored' status — in Tenable, this is the 'No CVSS' filter in the vulnerability list view; in OpenVAS, filter by `severity = 0.0` with no NVD reference. Retain these exports timestamped to establish the blind-spot surface at the moment of assessment.

Step 3: Supplement Enrichment Sources — Integrate at least one alternative enrichment source to cover the NVD gap. Evaluated options include VulnCheck KEV (expanded KEV coverage), OSV.dev (open-source ecosystem coverage), vendor-direct advisories via OVAL or SBOM feeds, and commercial threat intelligence platforms with independent CVSS scoring. Configure pipeline fallback logic to pull from secondary sources when NVD fields return null.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment: Execute IR plan to mitigate ongoing harm; here, containment means stopping the blind-spot from expanding by introducing compensating enrichment sources before additional unenriched CVEs accumulate in the pipeline

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives) — receive and operationalize vulnerability intelligence from multiple external organizations, not solely NVD, NIST SI-2 (Flaw Remediation) — flaw remediation requires accurate severity data; supplementing enrichment sources restores the scoring fidelity required to execute SI-2, NIST IR-4 (Incident Handling) — containment sub-phase of the incident handling capability applies here to prevent the gap from widening, NIST SA-9 (External System Services) — dependencies on external services (NVD API) must have contingency provisions; integrating OSV.dev or VulnCheck constitutes the required fallback, CIS 7.2 (Establish and Maintain a Remediation Process) — remediation process must remain functional even when primary enrichment source degrades; fallback logic is a process integrity requirement

Compensating: For a 2-person team with no commercial TI platform: (1) Configure a daily cron job using `curl` to pull from the OSV.dev API (`https://api.osv.dev/v1/query`) for your software inventory's package ecosystem (e.g., PyPI, npm, Maven). (2) Subscribe to vendor OVAL feeds directly — Red Hat OVAL at `https://www.redhat.com/security/data/oval/v2/`, Microsoft MSRC CVRF via `https://api.msrc.microsoft.com/cvrf/v2.0/`. (3) Write a Python script using the `requests` library to query NVD first, check if `metrics` is empty, and fall back to OSV.dev for severity data — store results in a local SQLite database as your interim enrichment cache.

Evidence: Before activating new enrichment sources, document the pipeline's current null-field rate by logging one full scan cycle's raw API responses from NVD with timestamps — this is your pre-integration baseline. After integration, log the first post-integration scan cycle outputs to confirm fallback logic is triggering correctly (OSV.dev or VulnCheck records appearing for CVEs where NVD returned empty `metrics`). Retain both logs to demonstrate that the gap was identified, measured, and remediated — required for audit trail continuity under NIST AU-3 (Content of Audit Records).

Step 4: Validate Pipeline Integrity — After integrating alternative sources, run a validation pass against a known CVE set to confirm enrichment fields are populating correctly across your toolchain. Test CVSS score

ingestion, CWE tagging, and CPE asset matching end-to-end. Establish a recurring check — weekly minimum — to detect future enrichment gaps before they compound.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Verify system and process integrity after remediation; confirm restored capability is functioning correctly before resuming normal operations and establish ongoing monitoring to detect recurrence

Controls: NIST SI-7 (Software, Firmware, and Information Integrity) — verify that enrichment data flowing through the pipeline is complete and untampered; null fields introduced by the NVD gap are an integrity failure mode, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — recurring weekly enrichment gap checks constitute the required ongoing review cadence, NIST CA-7 (Continuous Monitoring) — the recurring pipeline integrity check operationalizes continuous monitoring for the vulnerability enrichment process specifically, NIST IR-3 (Incident Response Testing) — validation against a known CVE set is a form of IR capability testing confirming the remediated pipeline performs as expected, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — process validation and recurring checks are explicit requirements of a documented vulnerability management process

Compensating: Build a validation test set of 10–20 CVEs: include 5 pre-April-15-2026 CVEs (known to have full NVD enrichment), 5 post-April-15-2026 KEV-listed CVEs (should still be enriched by NVD), and 5–10 post-April-15-2026 non-KEV CVEs (the gap candidates). Run your scanner or enrichment script against each and record which fields populate from which source. Automate the weekly check with a Python script that queries NVD for CVEs published in the prior 7 days, counts null `metrics` fields, and emails a summary if null rate exceeds a defined threshold (e.g., >20%). Store results in a dated CSV log for audit purposes.

Evidence: Retain the validation test run outputs — specifically, a diff between pre-integration and post-integration enrichment field population rates for the test CVE set. Document which CVEs now receive CVSS scores from fallback sources (OSV.dev, vendor OVAL, VulnCheck) vs. which remain unenriched after fallback — the latter are your residual blind spots requiring manual analyst triage. These validation records serve as evidence of due diligence for audit purposes under NIST AU-11 (Audit Record Retention) and demonstrate remediation efficacy if the gap is later cited in a compliance review.

Step 5: Update Prioritization Logic and Governance — Revise your vulnerability prioritization policy to explicitly acknowledge NVD's reduced scope. Define a documented fallback hierarchy for enrichment sources. Update SLAs for patch prioritization to account for delayed or absent CVSS data. Communicate the change to vulnerability management, SOC, and GRC teams. Communicate the change to vulnerability management, SOC, and GRC teams. Log the policy update for audit trail purposes.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Update policies, procedures, and detection capabilities based on lessons learned; share intelligence with relevant internal teams; improve organizational posture to prevent recurrence of the same gap

Controls: NIST IR-8 (Incident Response Plan) — IR plan must be updated to reflect the changed enrichment landscape, including the NVD scope restriction and the documented fallback hierarchy, NIST IR-1 (Policy and Procedures) — vulnerability prioritization policy revision and SLA updates constitute required policy and procedure maintenance, NIST SI-2 (Flaw Remediation) — SLA updates for patch prioritization when CVSS data is absent are a direct operationalization of the flaw remediation control, NIST AU-3 (Content of Audit Records) — logging the policy update with timestamp, author, and rationale satisfies the audit record content requirements for governance changes, CIS 7.2 (Establish and Maintain a Remediation Process) — the remediation process document must be updated to reflect the fallback source hierarchy and revised SLAs, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — the vulnerability management process document must explicitly acknowledge NVD's reduced scope effective April 15, 2026

Compensating: Use a version-controlled plain-text or Markdown policy document stored in a Git repository (free, auditable, timestamped) to capture the policy revision — commit message should reference the NVD policy change date (April 15, 2026) and the internal response date. For SLA tables, define explicit fallback tiers: (1) CVSS available from any source → standard SLA; (2) No CVSS but CVE is in CISA KEV → treat as Critical, 24-hour patch SLA; (3) No CVSS, not in KEV, internet-facing asset → treat as High, 72-hour review SLA; (4) No CVSS, not in KEV, internal asset

→ 30-day review SLA with documented risk acceptance. Distribute via email with read-receipt to VM, SOC, and GRC leads as the communication record.

Evidence: Preserve the pre-revision policy document (version-controlled diff or dated PDF export) alongside the revised version to demonstrate the governance change was deliberate and traceable. Retain communication records (email distribution list, meeting notes, or Slack/Teams export) showing that VM, SOC, and GRC teams were notified of the NVD scope change and updated SLAs. These records are the audit trail evidence required if a compliance auditor questions why unenriched CVEs received non-standard prioritization treatment after April 15, 2026 — they demonstrate the organization identified the gap, updated its process, and communicated the change in a documented and timely manner.

Detection Guidance

Direct detection of this issue is a pipeline audit problem, not a threat-hunting problem. To identify affected workflows: (1) Query your vulnerability management platform or ticketing system for open CVEs with null or missing CVSS base scores, empty CWE fields, or absent CPE strings published after April 15, 2026; these are candidates for the NVD enrichment gap. (2) Monitor NVD API responses for the 'vulnStatus' field value 'Not Scheduled'; any CVE returning this status will not receive enrichment under the new policy. (3) Check scanner console logs and SIEM enrichment job outputs for increased null-field rates or enrichment pipeline errors following the April 15 cutover date. (4) If your organization uses risk scoring models that auto-assign severity bands based on CVSS base score, audit for CVEs that have been assigned default or zero-score ratings since April 15; these may represent unscored CVEs silently deprioritized. No network-layer IOCs or endpoint behavioral indicators apply to this item; the risk is informational pipeline integrity, not active exploitation of a specific vulnerability.

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1203** — Exploitation for Client Execution
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-6** — Least Privilege
- **SA-22** — Unsupported System Components

OWASP-TOP10-2021

- **A06:2021** — Vulnerable and Outdated Components

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1203	Exploitation for Client Execution	Execution
T1068	Exploitation for Privilege Escalation	Privilege-Escalation

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/nist-limits-cve-enrichment-after-...	T3
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
NIST Prioritizes NVD Enrichment for CVEs in CISA KEV, Critical ...	https://www.securityweek.com/nist-prioritizes-nvd-enrichment-for-cv...	T3
CISA Adds Two Known Exploited Vulnerabilities to Catalog	https://www.cisa.gov/news-events/alerts/2026/04/14/cisa-adds-two-kn...	T1
NIST Updates NVD Operations to Address Record CVE Growth	https://www.nist.gov/news-events/news/2026/04/nist-updates-nvd-oper...	T1

Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-17 14:05 UTC by TJS Security Command Center