

# From Listing to Exploitation: Measuring KEV Entry Lag and Coverage Against Post-2024 Exploitation Evidence

**M. F. Mridha**

ORCID: 0000-0001-5738-1631

Department of Computer Science and Engineering, American International University-Bangladesh, Dhaka, Bangladesh

**Taeshik Shon**

ORCID: 0000-0003-1177-6405

Department of Cyber Security, Ajou University, Suwon, South Korea

**Correspondence:** M. F. Mridha · contact details held in the journal record

**Publication history.** Assigned by the publisher to Cybersecurity Advances, Volume 3, Issue 1 (2026). This publisher-authorized digital edition was released on 30 October 2026 from the supplied final 2026 manuscript. Review-stage notices were removed and journal typography, pagination, metadata, and accessibility were normalized; substantive scholarly content was preserved.

© 2026 the author(s). Published by AlphaTech Scholarly Press under the Creative Commons Attribution 4.0 International License (CC BY 4.0). No DOI is displayed unless and until registration is independently verified.

**Background:** CISA's Known Exploited Vulnerabilities (KEV) catalog is the most authoritative public statement that a vulnerability has been exploited — and, since 2024, the anchor of NIST's triage policy, with enriched analysis now promised for KEV entries within one business day of listing. Yet the catalog measures *agency decisions*, not exploitation itself, and the interval between the events that matter — CVE publication, KEV listing, and confirmed exploitation — has never been decomposed for the post-2024 period. **Objective:** This paper specifies a measurement framework for KEV entry lag and coverage, synthesizes the published record, and identifies the gaps that the 2026 enrichment policy leaves open. **Methods:** Documentary analysis of the KEV catalog's requirements and operations (2021–2026), the NVD prioritization policy of April 2026, and published exploitation-timing measurements; construction of a pipeline-lag decomposition and a gap-versus-mitigation matrix. **Results:** KEV listing is a lagged, decision-based signal: it requires an exploitation *determination* by CISA, not merely evidence, and its coverage is bounded by the catalog's statutory scope — non-federal, non-KEV high-risk vulnerabilities fall outside both the catalog and the new enrichment priority. We identify six residual gaps, of which the deepest is structural: the 2026 policy enriches the exploited minority within one business day while formally deprioritizing everything else, converting the enrichment gap into a permanent, policy-defined class. **Conclusions:** KEV-derived metrics should be reported as decision-lag measurements with explicit coverage bounds, complemented by predictive signals (EPSS) and community enrichment (ADP) — never as a complete map of exploitation.

**Keywords:** Known Exploited Vulnerabilities; KEV; exploitation intelligence; vulnerability prioritization; CISA; NVD enrichment; measurement; digital trust

**Contribution statement.** This paper makes four contributions: (1) a decomposition of the exploitation-intelligence pipeline into four measurable lags; (2) a source-verified timeline of the KEV–NVD policy coupling through the April 2026 enrichment decision; (3) identification of six residual coverage gaps, including the structural blind spot created by prioritized enrichment; and (4) reporting guidance for KEV-derived metrics.

## 1. Introduction

Few artifacts in vulnerability management carry more operational weight than CISA's **Known Exploited Vulnerabilities (KEV) catalog**: a binding list, established in November 2021, of vulnerabilities that the agency has confirmed as exploited [1]. Federal agencies must remediate KEV entries on fixed deadlines; the broader industry treats KEV inclusion as the strongest available public signal of real-world threat. And since 15 April 2026, the KEV catalog has acquired a second role: the anchor of NIST's triage policy for the National Vulnerability Database, under which CVEs appearing in the catalog are enriched — CPE, CWE, and CVSS analysis attached — within one business day of listing, while CVEs not in the catalog and published before March 2026 were moved to a "Not Scheduled" category [2][3].

The policy couples two datasets whose semantics differ. The KEV catalog answers *has CISA determined this is exploited?* — a determination that requires evidence gathering and carries legal weight. NVD enrichment answers *what are this vulnerability's technical properties?* The one-business-day promise therefore applies to a *decision*, and everything not in the catalog inherits the pre-2026 backlog condition permanently: CVEs published before March 2026 that were never enriched were moved to "Not Scheduled," to be considered "as resources allow" [2]. The result is a policy-defined two-tier vulnerability record: a small, fast, enriched exploited class, and a large, slow, or never-enriched remainder — the majority by count.

Understanding what this means for risk requires decomposing the timing of the underlying pipeline. Four events form the chain: a CVE is published; a vulnerability is (possibly) exploited; CISA determines and lists it in KEV; enrichment follows. Each transition is a measurable lag with its own distribution, and each has different consumers: defenders triaging need the *exploitation* signal early; compliance processes need the *KEV* signal; asset-matching tools need *enrichment*. Conflating them — as "KEV lag" reporting typically does — hides the policy question that the 2026 decision crystallized.

## 1.1 Research questions

**RQ1:** How does the KEV catalog's semantics differ from exploitation evidence, and what lags separate the pipeline's events? **RQ2:** How did the KEV–NVD policy coupling develop through the April 2026 enrichment decision? **RQ3:** Which coverage gaps survive the 2026 policy, and how severe are they? **RQ4:** How should KEV-derived metrics be reported and complemented?

## 1.2 Contributions

(1) A four-lag decomposition of the exploitation-intelligence pipeline (Section 4, Figure 2). (2) The verified KEV–NVD policy timeline through April 2026 (Section 3, Figure 1). (3) A six-gap residual analysis against six mitigation mechanisms (Section 5, Figure 3, Table 3) (RQ3). (4) Reporting guidance for KEV metrics (Section 6) (RQ4).

# 2. Background

## 2.1 The KEV catalog's semantics

The catalog's entry requirements are public: CISA lists a CVE when there is evidence of active exploitation in the wild and a clear remediation action — a *determination*, reviewed by analysts, not an automated prediction [1]. This gives KEV high precision (entries are exploited by definition, within the agency's evidence standard) but introduces structural lags: evidence must be observed, assessed, and confirmed. Published analyses of the catalog document that a substantial fraction of KEV entries correspond to vulnerabilities that were exploited years after disclosure — legacy vulnerabilities dominate the catalog's population — while newly disclosed CVEs typically enter only after exploitation has already been observed in incidents [1][6]. The catalog also binds to the U.S. federal remediation mandate (BOD 22-01), which shapes its scope decisions.

## 2.2 The 2024–2026 enrichment record

The KEV–NVD coupling was forged during the enrichment crisis. When NVD's analysis slowed in February 2024, the backlog grew past 18,000 CVEs; by September 2024, 72.4% of CVEs published since the slowdown remained unanalyzed — and notably, **46.7% of the KEVs added in that window were also unanalyzed**, despite the catalog's priority status [5]. CISA's Authorized Data Publisher (ADP) "Vulnrichment" service began supplementing CVSS and CWE data from July 2024 — a community-layer patch for the gap [6]. Processing recovered to pre-slowdown rates by March 2025, and NVD enriched approximately 42,000 CVEs in 2025 (45% more than any prior year), but submissions grew faster still — CVE submissions increased 263% between 2020 and 2025 — and the backlog was never cleared [2][3]. The April 2026 policy made the triage explicit: KEV-first enrichment within one business day, federal-software prioritization, and formal deprioritization of the pre-March 2026 backlog into "Not Scheduled" [2][3]. Crucially, NIST noted the backlog "does not include any CVEs in the KEV Catalog, as we have always prioritized those for enrichment" [2] — confirming that the enrichment gap was never a KEV-availability problem but a everything-else problem.

## 2.3 Related measurement work

Exploitation timing has been measured against public exploit repositories: the SEI's historical analysis of 75,807 CVEs found 4.1% associated with public exploit code within a year, with a median time-to-exploit of 2 days *given that one exists* [7]. Predictive signals (EPSS) and their stability across model versions are analyzed in the companion work in this issue [8]. What has not been published is a decomposition of the KEV-specific lags and the coverage bounds of KEV-anchored enrichment — the contribution of this paper.

### 3. Methodology

The study applies a three-component documentary methodology.

**Pipeline decomposition (RQ1).** The exploitation-intelligence pipeline was decomposed into four events and three lags: L1 (CVE publication → exploitation), L2 (exploitation → KEV listing), and L3 (KEV listing → enrichment). Each lag's semantics, observable proxies, and consumers are specified from the catalog's public requirements and NIST's enrichment policy [1][2][3].

**Policy-timeline verification (RQ2).** Every policy claim was verified against primary documents: the KEV catalog's published requirements [1], NVD's operational announcements (February 2024 through the April 2026 prioritization decision) [2][3][6], and the VulnCheck measurements of the backlog's KEV content [5]. The analysis is frozen at the April 2026 policy.

**Gap analysis (RQ3).** Six residual coverage gaps were derived from the pipeline decomposition and the policy text; six mitigation mechanisms were compiled from documented ecosystem responses. Coverage levels are qualitative author assessments tied to mechanism arguments (Table 3); their subjectivity is stated in Section 7.

### 4. The Pipeline and Its Lags (RQ1)

Figure 1 decomposes the chain. **L1 — publication to exploitation** is the lag predictive models attempt to forecast; the SEI measurement (median 2 days, mean 91 days, given an exploit eventually appears, with only 4.1% of CVEs receiving public exploit code within a year [7]) shows its skew: a small exploited minority with a fat tail. **L2 — exploitation to KEV listing** is the decision lag: it requires CISA to observe, corroborate, and confirm exploitation — an analytical process with legal consequences. **L3 — listing to enrichment** is, since April 2026, the one lag with a formal service-level objective: one business day for KEV entries [2][3].

| Lag                                | Definition                                 | Observable proxy                                                     | Primary consumer                          |
|------------------------------------|--------------------------------------------|----------------------------------------------------------------------|-------------------------------------------|
| L1: CVE publication → exploitation | Time until exploitation occurs in the wild | EPSS probabilities; exploit repositories (noisy); incident telemetry | Defenders triaging; researchers           |
| L2: exploitation → KEV listing     | CISA's determination and listing decision  | KEV listing date relative to earliest exploitation evidence          | Compliance processes; federal remediation |
| L3: KEV listing → enrichment       | NVD/ADP enrichment of the KEV entry        | Enrichment timestamps (≤1 business day from Apr 2026)                | Asset-matching tools; scanners            |

Table 2. The three exploitation-intelligence lags and their consumers.

The decomposition's value is diagnostic. When a defender asks "is this exploited?", the honest answer assembles three different signal classes: predictive (EPSS-style probabilities), decision-based (KEV), and observed (incident telemetry, exploit repositories). Each has a different lag profile, and each fails differently — EPSS is probabilistic and model-dependent, KEV is lagged and scope-bounded, observed exploitation is sparse. The 2026 policy makes L3 near-zero for the KEV class but does nothing for L1 and L2, which are properties of the exploitation itself and of CISA's assessment process.

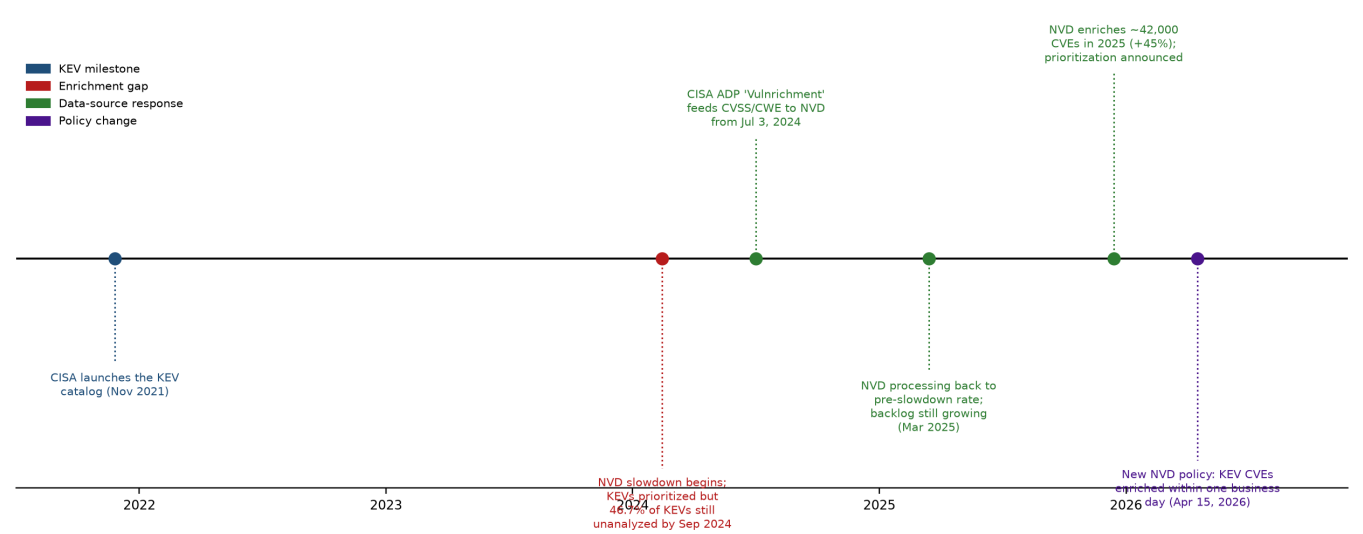


Figure 1. The exploitation-intelligence pipeline: CVE publication, enrichment, KEV listing, and confirmed exploitation — three lags with different semantics and consumers.

## 5. The Policy Coupling and Its Gaps (RQ2, RQ3)

### 5.1 The verified timeline

Figure 1 presents the verified KEV–NVD coupling. The catalog's priority status within NVD predates the 2026 policy — NIST stated in 2024 that all backlog KEVs had been addressed and new KEVs were processed on arrival [6] — and the April 2026 decision formalized that priority as a one-business-day service level [2][3]. The policy simultaneously formalized the deprioritization of everything else: CVEs published before March 2026 that lack enrichment moved to "Not Scheduled," and new non-KEV, non-federal CVEs are enriched only as resources allow [2][3].

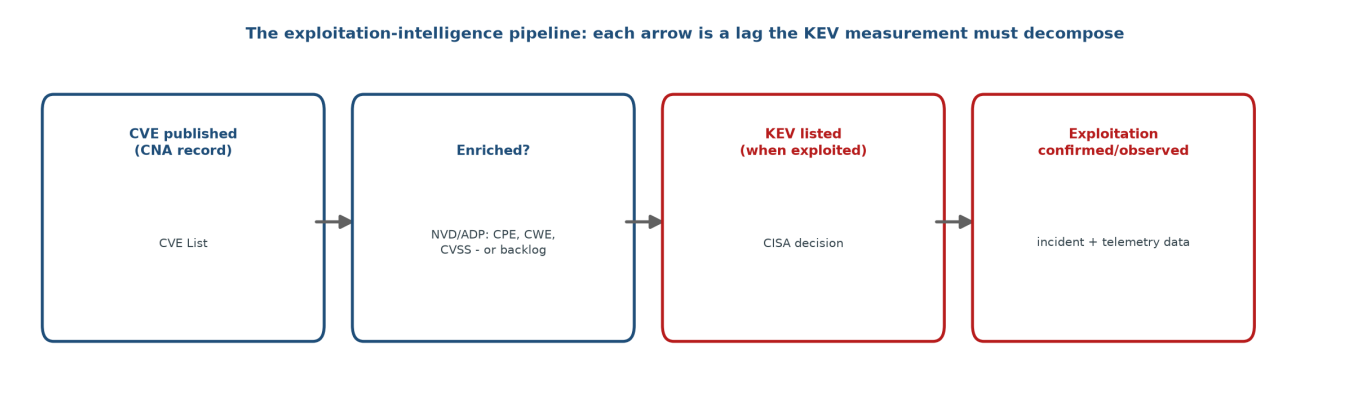


Figure 2. The KEV–NVD policy timeline, 2021–2026: catalog milestones, the enrichment-gap window, data-source responses, and the April 2026 prioritization decision [1][2][3][5][6].

| Policy/data event              | Date         | Content                                                                                     | Source |
|--------------------------------|--------------|---------------------------------------------------------------------------------------------|--------|
| KEV catalog established        | Nov 2021     | Binding exploited-vulnerability list with federal remediation deadlines (BOD 22-01)         | [1][4] |
| NVD enrichment slowdown begins | Feb 12, 2024 | Backlog of unenriched CVEs begins growing                                                   | [5][6] |
| ADP "Vulnrichment" support     | Jul 3, 2024  | CISA ADP supplies CVSS/CWE from the ADP layer                                               | [6]    |
| Processing recovery            | Mar 19, 2025 | Back to pre-slowdown rate; submissions grew 32% in 2024; backlog still growing              | [5][6] |
| Record 2025 enrichment         | 2025         | ~42,000 CVEs enriched (+45% over any prior year); still insufficient                        | [2]    |
| Prioritized enrichment policy  | Apr 15, 2026 | KEV entries enriched within one business day; pre-Mar-2026 backlog moved to "Not Scheduled" | [2][3] |

Table 1. The KEV-NVD policy timeline, 2021-2026 [1][2][3][5][6].

### 5.2 The six gaps

Figure 3 and Table 3 assess six residual gaps against six mitigation mechanisms. Three deserve emphasis.

**G2 — the frozen backlog.** Pre-March-2026 CVEs without enrichment are now in a formal "Not Scheduled" state — not a queue with a promise, but a category without a service level. The mitigation with real coverage is ADP community enrichment (the Vulnrichment model) [6]; the gap cell is partial because ADP data covers a subset of fields and arrives with its own quality variance.

**G4 — the non-KEV high-risk blind spot.** The policy's triage keys on two properties: KEV membership and federal software relevance. High-risk vulnerabilities in neither class — including many in the long-tail products that operational systems actually run — receive no enrichment priority. EPSS and exploit-signal correlation provide partial compensating coverage, but a probability signal cannot substitute for applicability data.

**G1 — lag without context.** KEV listing arrives when exploitation is confirmed, which is valuable for compliance but late for triage. The mitigation is to treat KEV as one signal among several — the register's finding is that no single source closes the loop (Table 3).

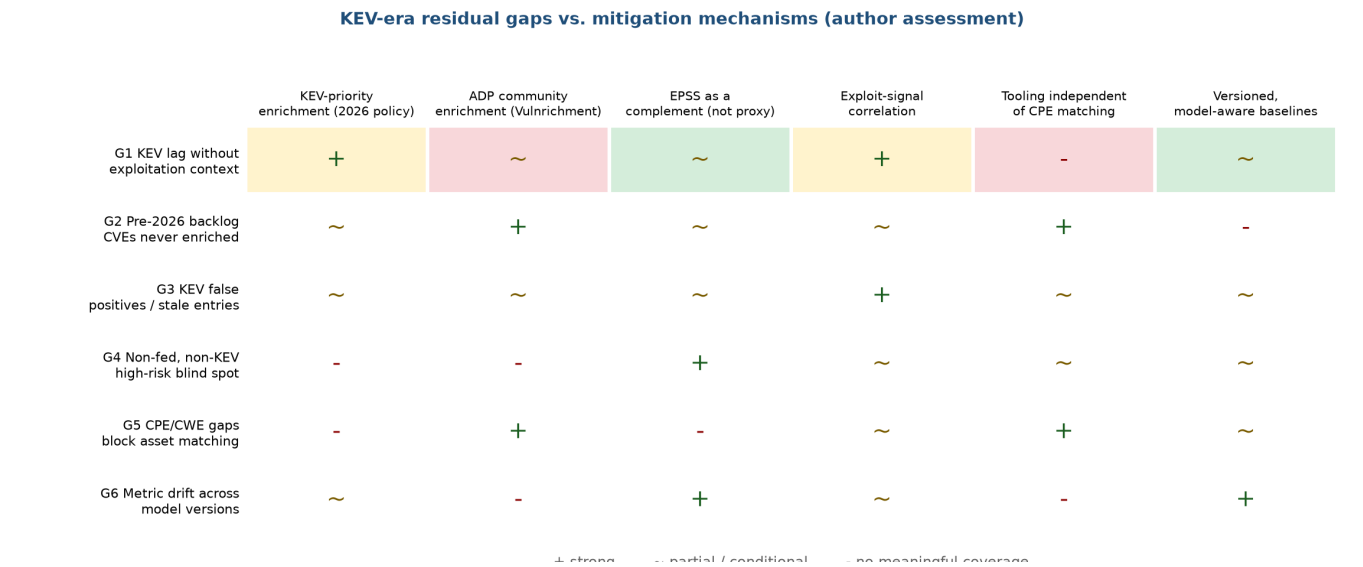


Figure 3. KEV-era residual gaps versus mitigation mechanisms (author assessment; register in Table 3).

| Gap                                          | Description                                                        | Strongest mitigation                                | Coverage note                                        |
|----------------------------------------------|--------------------------------------------------------------------|-----------------------------------------------------|------------------------------------------------------|
| G1 KEV lag without exploitation context      | Listing arrives at decision time, late for triage                  | Multi-signal fusion (EPSS + KEV + telemetry)        | Partial: no single source closes the loop            |
| G2 Frozen pre-2026 backlog                   | "Not Scheduled" category without a service level                   | ADP community enrichment (Vulnrichment model)       | Partial: subset of fields, quality variance          |
| G3 Stale/false KEV entries                   | Catalog entries whose exploitation has lapsed or was misattributed | Catalog review and removal process                  | Partial: CISA performs review; latency varies        |
| G4 Non-KEV, non-federal high-risk blind spot | High-risk CVEs outside the triage keys receive no priority         | EPSS + exploit-signal correlation as interim triage | Partial: probability signals lack applicability data |
| G5 CPE/CWE gaps block asset matching         | Enrichment gaps break CPE-based asset matching                     | Tooling not dependent on CPE (name-based matching)  | Partial: reduces precision                           |
| G6 Metric drift across model versions        | Prioritization metrics change as models update (see e001)          | Versioned, model-aware baselines                    | Partial: baseline discipline required                |

Table 3. KEV-era residual gaps, mechanisms, and coverage notes (author assessment).

6. Reporting Guidance (RQ4)

Four rules for KEV-derived metrics. (1) **Name the lag:** report "KEV listing lag" (L2) and "enrichment lag" (L3) separately; a blended "KEV age" metric conflates a decision with a data process. (2) **State the scope:** KEV coverage is bounded by CISA's determination practice and BOD 22-01's federal framing; report catalog coverage against the total CVE population as an explicit denominator [1]. (3) **Pair with predictive signals:** EPSS and KEV answer different questions (will it be exploited vs. has it been determined exploited); dashboards should show both with their distinct update semantics [8]. (4) **Audit the two-tier record:** track the "Not Scheduled" population's size and composition — it is now a policy-created class whose growth is a measurable indicator of the intelligence gap's trajectory [2][3].

7. Limitations and Threats to Validity

**Construct validity.** The four-lag decomposition is analytical; the boundaries between "exploitation observed" and "exploitation determined" are CISA's operational definitions, which may shift. **Internal validity.** Gap coverage levels are author assessments tied to mechanism arguments, not measurements. **External validity.** The analysis addresses the U.S. catalog-and-enrichment stack; other

national databases and private intelligence products have different semantics. **Reliability.** Policy documents and vendor telemetry are subject to revision; all claims are time-stamped. **Temporal scope.** Frozen at the April 2026 policy; its implementation performance (whether the one-business-day service level is met) is out of scope and should be measured.

## 8. Conclusion

The KEV catalog is the strongest public determination of exploitation — and the 2026 enrichment policy has made it the keystone of vulnerability-data triage, with one-business-day enrichment for the exploited class and formal deprioritization for the rest. This paper decomposed the resulting measurement problem into three lags with different semantics, verified the policy timeline that created the two-tier record, and identified six residual gaps — of which the structural one is that the policy enriches the exploited minority at business-day speed while the unenriched majority acquires a permanent category. KEV-derived metrics should be reported with their coverage bounds stated, complemented by predictive and community sources, and audited against the growing "Not Scheduled" population. A catalog of known exploited vulnerabilities is a map of where the fire has been confirmed — valuable, actionable, and explicitly not a map of the building.

## Declarations

**Funding.** This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

**CRedit contribution statement.** M. F. Mridha: conceptualization, exploitation-timeline analysis, writing – original draft. Taeshik Shon: validation, policy-timeline verification, writing – review & editing. (Corresponding author: M. F. Mridha.)

**Competing interests.** The authors declare no competing interests.

**Data and code availability.** No new datasets were generated; all policy and measurement claims trace to the cited primary documents [1][2][3][5][6][7].

**Ethics and dual-use.** Not applicable; the paper contains no offensive content.

**AI assistance declaration.** AI-based tools were used in a limited supporting capacity (literature search, figure preparation, and language editing); all research content, analysis, and conclusions were produced, reviewed, and verified by the authors, who take full responsibility for the work.

## References

- [1] Cybersecurity and Infrastructure Security Agency, "Known Exploited Vulnerabilities (KEV) Catalog," CISA, established Nov. 2021, updated continuously. [Online]. Available: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- [2] National Institute of Standards and Technology, "NIST Updates NVD Operations to Address Record CVE Growth," Apr. 2026. [Online]. Available: <https://www.nist.gov/news-events/news/2026/04/nist-updates-nvd-operations-address-record-cve-growth>
- [3] National Vulnerability Database, "CVEs and the NVD Process" (enrichment scope and prioritization), NIST, Apr. 2026. [Online]. Available: <https://nvd.nist.gov/general/cve-process>
- [4] Cybersecurity and Infrastructure Security Agency, "Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities," Nov. 2021 (updated 2022 as BOD 22-01 v2).
- [5] P. Garrity, "Danger is Still Lurking in the NVD Backlog," VulnCheck Blog, Sep. 30, 2024. [Online]. Available: <https://www.vulncheck.com/blog/nvd-backlog-exploitation-lurking>
- [6] National Institute of Standards and Technology, "NVD News" (ADP Vulnrichment support, backlog updates, Jul. 2024 et seq.). [Online]. Available: <https://nvd.nist.gov/itl/nvd/nvd-news>
- [7] J. Beerman, L. Allodi, and J. M. Spring, "Historical Analysis of Exploit Availability Timelines," in Proc. USENIX Workshop on Cyber Security Experimentation and Test (CSET '20), 2020. [Online]. Available: <https://www.sei.cmu.edu/library/historical-analysis-of-exploit-availability-timelines/>
- [8] J. Zhang, "Exploit Prediction Scoring System (EPSS) — reference implementation and model documentation," FIRST, 2023-2025. [Online]. Available: <https://www.first.org/epss/>