HACKING POLICY COUNCIL

Transformative changes needed for vulnerability infrastructure and the National Vulnerability Database

May 12, 2024

A key aspect of digital security is effective vulnerability management. With tens of thousands of vulnerabilities identified in hardware and software each year, and growing, it is a business and societal imperative to identify, assess, and mitigate vulnerabilities to safeguard systems against breaches and cyberattacks.[1] Vulnerability management is also increasingly a legal obligation for the private and public sectors under privacy and cybersecurity regulations.

At the same time, it is apparent that infrastructure supporting vulnerability management requires significant improvements to meet contemporary demands. Specifically, the National Vulnerability Database (NVD), a key resource for organizations for sourcing vulnerability information, is in urgent need of modernization. The NVD suffers from several longstanding administrative and technological challenges that have recently led to a serious degradation in NVD's operations.[2] The unsustainable path of this widely used tool creates substantial risks for organizations that seek to secure their digital assets against the latest vulnerabilities.

The Hacking Policy Council urges prompt action to transform the NVD to be more efficient, accurate, comprehensive, and scalable. In the absence of significant modernization and support of the NVD, organizations should consider direct engagement with alternative vulnerability information sources for more reliable and up-to-date sources, such as the CVE Program. The Hacking Policy Council urges against restructuring the NVD in a form that creates conflicts of interest or unnecessary bureaucratic hindrances. Policymakers and the security community must consider how to modernize shared vulnerability indexing and management infrastructure to meet anticipated needs in a future with increased prevalence of embedded software and artificial intelligence (AI).

I. Vulnerability infrastructure overview

The NVD serves as a repository and distribution point for software and hardware flaws that can compromise computer security.[3] It is arguably the world's most widely used vulnerability database. The NVD is presently operated by the National Institute of Standards and Technology (NIST), and was partially funded by the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security (DHS).

Many security vulnerability management activities rely on the index of known vulnerabilities compiled in NVD, referred to as Common Vulnerabilities and Exposures (CVEs), making the NVD a key part of the information supply chain. Security tools and services may draw CVEs from the NVD to help enable organizations make risk-based decisions about vulnerabilities. The NVD also enables users of digital products to check for known

[1] CVE Program, Metrics, Published CVE Records, https://www.cve.org/About/Metrics (last accessed May 1, 2024). Published CVE records have rapidly increased each year since 2016, with 28,961 CVE records published in 2023.
[2] NIST, NVD Program Announcement, Apr. 25, 2024, https://nvd.nist.gov/general/news/nvd-program-transition-announcement.
[3] NIST, National Vulnerability Database, Apr. 25, 2024, https://nvd.nist.gov.

issues with the product. Such tools are critical to helping organizations identify and triage vulnerabilities for mitigation, develop software securely, and manage supply chain risks. CVE Identifiers (CVE IDs) have become the standard means for identifying known vulnerabilities in software, allowing users to quickly access information about a problem across multiple information sources.[4]

The primary source of NVD's vulnerability information is the CVE List. According to NIST, the NVD processes the CVE List every hour to ingest new CVE information.[5] The CVE List is published by the CVE Program, which is maintained by the nonprofit MITRE Corporation with sponsorship from CISA. Newly identified vulnerabilities may be submitted to CVE Program participants, which may then assess the vulnerability and reserve a CVE ID. The CVE Program participant adds details of the CVE entry, including affected products, root cause, and impact severity, and may then submit the information to the CVE Program.[6] CVE Numbering Authorities (CNA) approved by MITRE assign CVE IDs to the vulnerabilities, and may add Common Vulnerability Scoring System (CVSS) scores and other data such as Common Weakness Enumeration (CWE) and Common Platform Enumeration (CPE). The CVE Program then publishes the CVE Record to the CVE List as an identifiable and trackable vulnerability.[7]

The CVE Program provides an API to allow external partners to automatically retrieve information on vulnerabilities for free.[8] The NVD consumes the content of the CVE Records through the CVE Program API.[9] When the NVD obtains CVE Records, NVD personnel manually "enrich" each CVE Record with metadata, including affected products, CVSS scores, and patching status – often duplicating the work of the CVE Program – before republishing the CVE Records in the NVD. The NVD then acts as a centralized distribution point with a search function. The NVD also provides its own API for free external use.[10]

Many vulnerability management tools and services are configured to draw from the NVD through its API, although the CVE Program API is also available as an option. Notably, CVE Program activities – including CVE Records, CVSS scoring, and the CVE Program API – take place independently of the NVD. CNAs are equipped to identify, analyze, and score CVEs in standard structured data formats relatively quickly. These activities continue to take place during the recent collapse in NVD operations.

II. Longstanding issues led to NVD's collapse

The NVD has fallen short of vulnerability management community needs, recently culminating in a sharp reduction in operations.[11] Since Feb. 15, 2024, the NVD almost completely stopped enriching the vulnerabilities it indexes.[12] Instead, thousands of vulnerabilities appear on the NVD without critical metadata such as affected

---

[4] Cybersecurity Coalition, Policy Priorities for Coordinated Vulnerability Disclosure and Handling, pg. 14, Feb. 25, 2019, https://www.cybersecuritycoalition.org/reports/white-paper-policy-priorities-for-coordinated-vulnerability-disclosure-and-handling/.

[5] NIST, National Vulnerability Database General FAQs, Mar. 19, 2024, https://nvd.nist.gov/general/FAQ-Sections/General-FAQs#faqLink0.

[6] CVE Program, CVE Record Lifecycle, https://www.cve.org/About/Process (last accessed May 2, 2024).

[7] CVE Program, CVE Numbering Authorities, https://www.cve.org/ProgramOrganization/CNAs (last accessed May 2, 2024).

[8] CVE Program, CVE Services, https://www.cve.org/AllResources/CveServices (last accessed May 2, 2024).

[9] CVE Program, Program Relationship with Partners, https://www.cve.org/ProgramOrganization/ProgramRelationshipwithPartners (last accessed May 2, 2024).

[10] NIST, National Vulnerability Database, CVE API, Mar. 19, 2024, https://www.cve.org/AllResources/CveServices.

[11] NIST has communicated little of substance regarding this development, despite being aware of the impending shutdown. NIST, NVD Program Announcement, Apr. 25, 2024, https://nvd.nist.gov/general/news/nvd-program-transition-announcement.

[12] Between Feb. 15 and Apr. 9, 2024, approximately 5,799 newly published CVEs were unanalyzed by NVD. Jonathan Munshaw, What's the deal with the massive backlog of vulnerabilities at the NVD?, Cisco Talos, Apr. 19, 2024, https://blog.talosintelligence.com/nvd-vulnerability-backlog-the-need-to-know.

products, CVSS scores, and patching status.[13] This lapse drew the alarm of numerous cybersecurity professionals, who issued an urgent letter to the U.S. Congress and Secretary of the Department of Commerce requesting immediate restoration of NVD operations and long term modernization.[14]

While the collapse of NVD activities is recent, its problems are not new. The NVD lagged behind in processing thousands of vulnerabilities for several years.[15] A major cause of this backlog is, as noted above, NVD personnel performing redundant work by manually reviewing every CVE entry and re-scoring vulnerabilities, typically ignoring the information already provided by the CNAs through the CVE Program. This inefficiency delays processing vulnerabilities and creates conflicts when NVD re-scoring differs from that of the CNAs. For example, NVD re-scored vulnerabilities for operational technology have repeatedly been criticized as prone to inaccuracy. When CNAs score a vulnerability, they often have greater access than NVD to the vendor and code of the affected product. NVD has not implemented recommendations to cease redundant work or to feature both a vendor score and an NVD score.

NVD also had budgetary challenges. NIST, which operates NVD, suffered a budget cut of more than 10 percent in 2024, despite rapidly growing responsibilities related to cybersecurity and AI.[16] Resources for the NVD were further reduced in 2024 by "a change in interagency support" in which CISA withdrew funding from NVD.[17] CISA's withdrawal of support was prompted in part due to NVD's inefficient approach, as well as erroneous budgetary classification of NVD as a federally funded research and development center (FFRDC).

It should be noted that the CVE Program is also under-resourced and likewise grapples with the growing volume and diversity of reported vulnerabilities.[18] The CVE Program, operated by the MITRE Corporation, is funded primarily on short-term federal contracts with widely fluctuating allocations and scheduling.[19] As the source of CVEs for the NVD, disruption or instability in the CVE Program would have a significant impact on vulnerability management and the viability of the NVD.

III. Hacking Policy Council Recommendations

The ongoing slowdown of NVD hampers critical security activities such as vulnerability scanning and secure software development. This elevates the risk that organizations' vulnerability management processes will operate on outdated or incomplete information, resulting in missed vulnerability identifications or prioritizing the wrong vulnerabilities for remediation. In turn, this elevates the risk of breach or malicious exploitation of a vulnerability, which can harm individuals and subject organizations to regulatory consequences.

---

[13] Kevin Poireault, NIST National Vulnerability Database Disruption Sees CVE Enrichment on Hold, Infosecurity Magazine, Mar. 15, 2024, https://www.infosecurity-magazine.com/news/nist-vulnerability-database.

[14] Open Letter from Cybersecurity Professionals to the U.S. Congress and Secretary of Commerce, Apr. 12, 2024, https://docs.google.com/document/d/1y6JXhh52b1OMxLMQyl_WH0R2-85iYEBzjSm_fhv8-GY/edit.

[15] By one March 2024 estimate, approximately 100,000 vulnerabilities were not included in the NVD. Flashpoint, Global Threat Intelligence Report, pg. 8, Mar. 2024, https://go.flashpoint.io/2024-global-threat-intelligence-report-download.

[16] Cat Zakrzewski, This agency is tasked with keeping AI safe. Its offices are crumbling., Washington Post, Mar. 6, 2024, https://www.washingtonpost.com/technology/2024/03/06/nist-ai-safety-lab-decaying.

[17] NIST, NVD Program Announcement, Apr. 25, 2024, https://nvd.nist.gov/general/news/nvd-program-transition-announcement.

[18] Sean Lyngaas, House panel rips CVE contracting and oversight policies, Cyberscoop, Aug. 27, 2018, https://cyberscoop.com/cve-mitre-house-energy-and-commerce-committee.

[19] Letters from the Hon. Greg Walden, Hon. Gregg Harper, Hon. Marsha Blackburn, Hon. Robert E. Latta, Committee on Energy and Commerce, US House of Representatives, to MITRE Corp. and the U.S. Department of Homeland Security, Aug. 27, 2018, pg. 3, https://www.documentcloud.org/documents/4788036-082718-DHS-Recommendations-for-CVE-Program.html.

The NVD's disruption occurs at a time when there is an explosion of identified vulnerabilities, which is anticipated to continue growing as complex software and AI are increasingly embedded in products and services. Congressional leaders recently introduced bipartisan legislation that would require NIST and CISA to update the NVD and CVE Program to incorporate AI vulnerabilities, though the legislation does not provide NIST or CISA with any additional resources or funding to do so.[20]

The Hacking Policy Council recommends the following:

1. **Restore NVD operations immediately.** Because so many security tools and activities are presently configured to rely on the NVD, restoring NVD operations is necessary to minimize disruption in the short term. However, providing NVD with more funding while failing to streamline its processes and modernize its technologies will not establish the long-term reliability and value needed for ecosystem cybersecurity. This funding should also require that NVD eliminate redundant work. In the absence of a clear inaccuracy, NVD should act as a passthrough and make CVE records available as they are provided, without overwriting information provided by CNAs or CISA's "Vulnrichment Program."[21]

2. **Empower the CVE Program to serve as a central source of vulnerability information.** Given NVD's longstanding challenges and ongoing disruption, industry should not depend solely on the NVD for vulnerability information.[22] While CVE users should not be forced to interrogate multiple databases to obtain comprehensive vulnerability information, the CVE Program should be empowered and recognized as a consensus alternative to the NVD.[23] The NVD only contains CVEs that have been published to the CVE List.[24] As noted above, the CVE Program already serves as the primary source of NVD's vulnerability information, and already provides record formats that support vital elements like CVE numbers, CVSS scores, and other data.[25] The CVE Program should designate additional CNAs to further expand its ability to identify and publish vulnerabilities as CVE Records, and the CVE Program should continue to encourage all CNAs to enrich CVE Records. The security community should consider taking advantage of the CVE Program API to obtain CVEs directly from the CVE Program, particularly during disruptions to NVD operations.

3. **Impose technological and process changes.** Greater reliance on automation is vital to address the current NVD CVE backlog and prevent new backlogs from forming as vulnerability reports grow. Where the CVE Program has already provided CVEs with CVSS scores and other data, NVD should not manually re-enrich the CVE Records. CISA's recently announced Vulnrichment program tests and enriches vulnerabilities in public CVE records where data fields have not already been filled by the originating

[20] Senator Mark Warner, Warner, Tillis Introduce legislation to Advance Security of ARtificial Intelligence Ecosystem, May 1, 2024, https://www.warner.senate.gov/public/index.cfm/2024/5/warner-tillis-introduce-legislation-to-advance-security-of-artificial-intelligence-ecosystem.
[21] Open Letter from Cybersecurity Professionals to the U.S. Congress and Secretary of Commerce, Apr. 12, 2024, https://docs.google.com/document/d/1y6JXhh52b1OMxLMQyl_WH0R2-85iYEBzjSm_fhv8-GY/edit.
[22] Saeed Abbasi, De-risking Your Organization in Spite of NVD Delays, Qualys, Mar. 13, 2024, https://blog.qualys.com/product-tech/2024/03/13/de-risking-your-organization-in-spite-of-nvd-delays.
[23] Kevin Townsend, CVE and NVD - A Weak and Fractured Source of Vulnerability Truth, Security Week, Apr. 3, 2024, https://www.securityweek.com/cve-and-nvd-a-weak-and-fractured-source-of-vulnerability-truth/.
[24] NIST, National Vulnerability Database General FAQs, Mar. 19, 2024, https://nvd.nist.gov/general/FAQ-Sections/General-FAQs#faqLink0.
[25] CVE Program Blog, New CVE Record Format Enables Additional Data Fields at Time of Disclosure, Apr. 27, 2024, https://medium.com/@cve_program/new-cve-record-format-enables-additional-data-fields-at-time-of-disclosure-82eef1d4035e.

CNA.[26] The Vulnrichment program further reduces the incentive for NVD to rewrite CVE entries. While NVD may be motivated to prevent inaccurate vulnerability descriptions or improper scoring, the CVE Program has access to more reliable data and is typically in a better position to evaluate the vulnerability. Any inaccurate CVE descriptions or scoring can be readily traced back to the assigning CNA, which is identified in the CVE Record. Spot audits, automated checks, marketplace transparency, and community feedback are more scalable mechanisms to oversee CVE accuracy. In addition, NVD must make more consistent use of structured file formats such as JSON5, which are supported by the CVE Program and increasingly used in the vulnerability management community.

4. **Establish sustained funding for vulnerability infrastructure.** Sustained resources are needed to provide the stability necessary for long-term planning and effective use of CVEs for security activities. The NVD and CVE Program should be established as part of a dedicated Program, Project, or Activity (PPA) with a line item in DHS' annual budget.[27] Congress should allocate necessary funds to DHS for this purpose. Funding should be contingent on imposing the technological and process changes described above. The CVE Program should be prioritized given the dependence of the NVD on the CVE Program.

5. **Reconsider NIST's proposed consortium model.** In the wake of NVD's collapse, NIST announced it would seek to transition the NVD to a public-private consortium.[28] This consortium model runs a strong risk of pay-to-play participation and conflicts of interest. NIST officials stated that candidates for the consortium must sign a Cooperative Research and Development Agreement (CRADA) with NIST and potentially be charged a membership fee. The consortium would have a steering committee.[29] Relying on membership fees to operate the NVD risks compromising its independence. In addition, if NVD continues to manually re-score vulnerabilities, the consortium model could put private company members in the position of prioritizing or assigning severity scores to competitors' vulnerabilities. At minimum, any consortium must establish robust governance mechanisms to prevent such issues, but we believe either NIST or CISA's Vulnerability Division are more appropriate hosts for NVD.[30]

* * *

The Hacking Policy Council urges swift action to avoid a preventable cybersecurity crisis due to failure to address the long-term administrative, technological, and resource challenges of vulnerability management infrastructure.

For more information, contact Harley Geiger, Hacking Policy Council Coordinator, at

HLGeiger@Venable.com.

---

[26] This includes adding stakeholder-specific vulnerability categorization (SSVC) to new and recent CVEs, as well as CVSS, CWE, CPE, and other information. CISA states that it will not overwrite information provided by the originating CNA. CISA, CISA Vulnrichment, May 8, 2024, https://github.com/cisagov/vulnrichment.

[27] Letters from the Hon. Greg Walden, Hon. Gregg Harper, Hon. Marsha Blackburn, Hon. Robert E. Latta, Committee on Energy and Commerce, US House of Representatives, to MITRE Corp. and the U.S. Department of Homeland Security, Aug. 27, 2018, pg. 5, https://www.documentcloud.org/documents/4788036-082718-DHS-Recommendations-for-CVE-Program.html.

[28] NIST, NVD Program Announcement, Apr. 25, 2024, https://nvd.nist.gov/general/news/nvd-program-transition-announcement.

[29] Kevin Poireault, NIST Unveils New Consortium to Operate National Vulnerability Database, Infosecurity Magazine, Mar. 28, 2024, https://www.infosecurity-magazine.com/news/nist-unveils-new-nvd-consortium.

[30] CISA, as a root CNA, is already performing many types of work that NVD reproduces. We do not recommend tying NVD to JCDC, as JCDC's effectiveness is questionable.