April 12, 2024

Sent via Electronic Mail

Chairwoman Maria Cantwell
Ranking Member Ted Cruz
Committee on Commerce, Science, and Transportation
United States Senate

Chairman Frank Lucas
Ranking Member Zoe Lofgren
Committee on Science, Space, and Technology
United States House of Representatives

Chairwoman Patty Murray
Vice Chairwoman Susan Collins
Committee on Appropriations
United States Senate

Chairman Tom Cole
Ranking Member DeLauro
Committee on Appropriations
United States House of Representatives

The Honorable Gina Raimondo
Secretary of Commerce
United States Department of Commerce

An Open Letter from Cybersecurity Professionals to the U.S. Congress and Secretary of Commerce

A cybersecurity crisis in waiting: On the Need to Restore and Enhance Operations with the National Vulnerability Database

To the Honorable Members of the United States Congress and the Honorable Gina Raimondo,

We, the undersigned, are cybersecurity researchers and practitioners who have diverse expertise in vulnerability management. In recent years, vulnerability exploitation has resulted in significant societal impacts, including major ransomware attacks on critical infrastructure. Run by the National Institute of Standards and Technology (NIST), the National Vulnerability Database (NVD) is a critical tool in defending against these threats, and its continued availability is essential for national security. We are deeply concerned by recent changes which threaten to cripple the NVD, and urge you to investigate thoroughly and prioritize modernization of the database.

NVD plays a vital role in the information supply chain for security vulnerability management worldwide. Our community uses CVE information distributed by NVD to find, prioritize, and fix vulnerabilities in critical systems before attackers try to exploit them. Many organizations rely solely on NVD provided severity scores to prioritize vulnerabilities and align remediation timelines accordingly. Around February 15 of this year, we observed an absence of critical metadata from new vulnerabilities listed in the NVD, which is essential for cybersecurity functions in organizations worldwide. This shutdown has disrupted essential resilience efforts across the public and private sectors.

We urge you to expeditiously investigate the ongoing issues with the NVD and ensure NIST has the necessary resources to restore operations immediately, as well as lay the groundwork for critical improvements to the service. This includes, but is not limited to:

- Immediately restore NVD operations. To minimize disruption to vulnerability management tools during NVD's disruption, we recommend stopgap processes for NVD to act as a passthrough of CVE Numbering Authority (CNA) data without re-scoring or duplicating the work of CVE programs, except in cases of clear inaccuracies in CNA-provided data.
- Establish a plan, with clear timelines and accountability, to improve NVD processes and operations. These must include addressing the backlog of vulnerabilities at NVD, lack of support for standard file formats, and redundant or conflicting vulnerability scoring. This plan should be developed openly with public and private stakeholder input with a public comment period.
- Investigate the lack of transparent communication from NIST regarding regression in NVD operations for the period of February 15, 2024 through March 25, 2024.
- Consider the establishment of sustained funding to provide reliable resources for NVD daily operations without conflicts of interest.
- The NVD should be treated as an essential service and as “Critical Infrastructure”. To minimize the impact of funding related slowdowns, we think it’s important for the NVD to continue running through government shutdowns and other disruptions that would otherwise impede the critical services it provides.
- Keep the NVD independent. While industry collaboration with NIST and the NVD should be encouraged, a single entity should clearly own and operate NVD, given its critical role as a source of truth for the federal government.

Beginning with Executive Order 14028 the United States Government has pursued an ambitious agenda to raise the bar for cybersecurity capabilities across multiple dimensions. NVD operations are a core building block of these efforts, and the current state of NVD operations is hindering our progress. This situation must be corrected with a sense of urgency appropriate to the broader strategic imperative of securing our systems infrastructure.

We respectfully request your immediate attention to this matter and look forward to working with you to ensure the NVD remains a reliable source of vulnerability information for the cybersecurity community.

Sincerely,
Dan Lorenc, CEO Chainguard
Nic Chaillan
Omkhar Arasaratnam
Chris Hughes
Rob Gil
Patrick Garrity
John Amaral
Marta Rybczynska
Tyler Young
Jeffrey Martin, VP Mend.io
Susan Jenkins, VP Foxguard Solutions, INC
Ian Riopel, CEO Root.io
Maor Kuriel
Anthony Bettini
Brendan O’Leary
Tyler Waldo
Varun Talwar
Dom Lombardi
Elias Levy
Andrew Pollock
Preyansh Matharoo
Om Mahida
Marcel Stör
Maxime Gréau
Yotam Perkal
Nick Waringa
Richard Tweed
Tim Pletcher
Brian Levine
Maryann Horst
Kiran Chinnagangannagari
Joshua Scarpino
Tony Turner
Matt Dillon
Curtis Yanko
Alfredo Hickman, CISO Obsidian Security
Murali Mallina, Softrams LLC
Scott A. Jones
Yamil Lugo
Eric R Allard

Matthew Moore
Rajat Pani
Angelo Aquino
Ed Drabek
François Proulx
Andrew Alaniz
Jelai Wang
David T. Jones
Mohamed AbuMuslim
Zsolt Nemeth
Jonathan Acosta-Torres
Ryan Cribelar
Kyle Kelly
Kaylin Trychon
Marek Counts

Cc:
Majority Leader Chuck Schumer
Minority Leader Mitch McConnell
Speaker Mike Johnson
Minority Leader Jefferies
The Honorable Gary Peters
The Honorable Rand Paul
The Honorable Cathy McMorris Rodgers
The Honorable Frank Pallone, Jr.
The Honorable James Comer
The Honorable Jamie Raskin