CENTER FOR
CYBERSECURITY
POLICY AND LAW

ENSURING THE LONGEVITY OF THE CVE PROGRAM

The CVE program is vital to cybersecurity but questions around funding have raised questions about its future.

By Ari Schwartz and Jessie Shen

JULY 2025

INTRODUCTION

Since 1999, the Common Vulnerabilities and Exposures (CVE) program has been a cornerstone of software vulnerability management worldwide. Following recent federal overhauls and significant funding changes, CVE has circulated the headlines and attracted attention to its uncertain future. Combined with long-standing concerns over a lack of investment and innovation in the way the CVE program operates, many security experts are now seeking alternatives to CVE, or looking at possible modifications to the current program to ensure it remains a viable and effective standard.

This paper provides a framework for those experts looking to preserve the most useful aspects of the CVE program. The report provides background on the program and starts a discussion about what questions some of these new proposals should answer.

This paper aims to define challenges with the CVE program before seeking solutions. Any modifications to the program should unite the cybersecurity community, rather than create factions that will complicate the preservation of 25 years of standardization.

CVE HISTORY - 25 YEARS OF STANDARDIZING VULNERABILITY MANAGEMENT

Software vulnerabilities are flaws or weaknesses in computer programs that can be exploited to cause unintended behavior or security risks. Before 1999, the software vulnerability space lacked standardization and interoperability. To manage software vulnerabilities, each security vendor, research group, and agency would maintain its own proprietary vulnerability database. Upon coming across a software vulnerability, IT staff and security researchers would manually cross-reference alerts over diverse vendor tools with different naming conventions to determine if the discovered vulnerability represented an already existing one. The fragmented vulnerability space obfuscated the ability for vulnerability information to be shared across organizations and industries globally.

In January of 1999, David Mann and Steven Christey Coley from the Mitre Corporation (MITRE), an American 501(c)(3) nonprofit organization, highlighted the challenges of a fragmented vulnerability landscape, publishing the white paper "Towards a Common Enumeration of Vulnerabilities."[1] They discussed three main roadblocks to interoperability: inconsistent naming conventions, slightly differing vulnerability documentation, and multiple evolving perspectives of the same vulnerability.

By September of 1999, Mann and Christey's concept was realized; their initial proposal of a standardized vulnerability database, the Common Vulnerability Enumeration system, came to

[1] https://cve.mitre.org/docs/docs-2000/cerias.html

fruition with the creation of 321 records. A 19-member working group of representatives from tool vendors, MITRE, academia, and the broader security industry was also formed, developing into the "CVE Editorial Board" now known as the CVE Board.

Common Vulnerability Enumeration evolved into Common Vulnerabilities and Exposures, now simply abbreviated as CVE. The CVE List is a publicly available catalog of all published security flaws. It standardized software security bug tracking and reporting worldwide, helping IT professionals coordinate their efforts to secure software systems. CVE identifiers (CVE IDs) provide a uniform naming convention for users to reliably recognize unique vulnerabilities. CVE Numbering Authorities (CNAs) assign CVE IDs to vulnerabilities, which then make their way onto the CVE List.

Although the structure, governance, and funding of CVE has evolved over the past 25 years, CVE has always relied on a public-private partnership. CVE is currently maintained by the Homeland Security Systems Engineering and Development Institute, a federally funded research and development center (FFRDC) operated by MITRE.

Before the Department of Homeland Security (DHS) was created in 2003, CVE was sponsored under a multi-agency funding model by various organizations, including the Defense Information Systems Agency, the Intelligence Community, and Department of Energy. Later, the DHS Science and Technology Directorate (S&T) sponsored the FFRDC supporting the CVE program. The program is currently funded by the Cybersecurity and Infrastructure Security Agency (CISA).

At first, MITRE acted as the sole CNA tasked with assigning all CVE IDs under the review of the CVE Board. In October of 2016, the program had 24 vendors designated as CNAs — but it needed more partners to scale. Adopting a federated model enabled the CVE program to thrive. The CVE Board expanded existing roles and onboarded more partner organizations, requiring CNAs to publish their own CVE Records consistent with the newly published CNA Rules.

This system gave the responsibility of CVE ID assignment and record publication to those with the most knowledge of the vulnerabilities — those closest to the product. This change in CVE structure was a win-win situation for both MITRE and its vendors. Distributing the workload enabled CVE to scale while incentivizing organizations to become CNAs with the promise of having control over vulnerability publication release. In addition, CNA expansion led to a significant increase in identified vulnerabilities.

Now, CVE has an impressive 459 CNAs spanning 40 countries. As the number of CNAs increased, the CVE Board created two new roles: Top-Level Roots and Roots. There are two Top-Level Roots, MITRE and CISA, that report directly to the CVE Board and are responsible for governing their respective CNA and Root hierarchies. Each Root is responsible for recruiting, training, and governing at least one CNA or other Root. While Roots are managerial, CNAs are operational, assigning IDs and publishing CVE Records.

In 2005, the National Institute of Standards and Technology (NIST) launched the National Vulnerability Database (NVD). With the help of DHS funding, the Internet Category of Attack Toolkit (ICAT) underwent a major facelift and was rebranded to the first iteration of the NVD.

Serving a similar purpose to the NVD is the EU Vulnerability Database (EUVD). Under the EU's NIS2 Directive, a component of which included having Member States create policies for vulnerability management, the EU brainstormed a version of its own CVE List. Reducing its dependency on U.S. tools and taking a step toward technological sovereignty, on May 13, 2025, the EU officially launched the beta version of the EUVD.[2]

Think of CVE as the backbone to vulnerability management — basic vulnerability information first appears in the CVE List — only then can the NVD and EUVD import that information about each newly discovered vulnerability and augment it with additional data such as severity scores. This process is called enrichment, enabling agencies such as NIST to re-package and display vulnerability information in a manner that is better suited to serve U.S. government and agency needs. CVE also powers the ability for cybersecurity tools to automate for cyber defense.

CVE IN THE HEADLINES

Throughout its 25 years of existence, CVE has faced a few funding scares. This year's federal overhaul has raised the most concern by the global cybersecurity community.

Yosry Barsoum, MITRE's vice president, alerted CVE Board members with one day's notice that the U.S. government's funding contract with MITRE was set to expire on April 16, 2025. The leaked memo alarmed the cybersecurity community. If the government did not renew its contract with MITRE within the next 36 hours, CVE would be in jeopardy. Even a temporary service break would degrade the effectiveness of the CVE List and the ability for vulnerability management professionals to efficiently respond to cyber incidents.

At the 11th hour, the DHS' contract with MITRE was reinstated, temporarily preserving CVE. Although CVE is safe until at least March 16, 2026, the last-minute reprieve caused experts in the cybersecurity space to come forward with alternatives to the fully U.S.-government-funded program. On April 16th, the Global CVE Allocation System (GCVE), operated by the Computer Incident Response Center Luxembourg (CIRCL), was born as a decentralized approach to CVE.[3] It uses a separate ID system and allows for GCVE Numbering Authorities (GNAs) to work independently. This is not the first time a separate vulnerability management system has been created. The China National Vulnerability Database (CNNVD) was launched in 2009 and also uses an independent ID system.[4] Although

[2] Although related, the NVD and EUVD are not to be confused with CVE. We raise it here because the CVE ID is used as the identifier for both; separating the use of the CVE ID could cause fragmentation.

[3] https://gcve.eu/

[4] https://www.cnnvd.org.cn/

vulnerabilities shown in the CNNVD may have both a CNNVD ID and a CVE ID if recognized by both databases, it is not a direct one-to-one mapping.

Following the reinstatement, members of the CVE Board launched the CVE Foundation, a nonprofit organization proposing a new form of governance to the current program.[5] The CVE Foundation is working to modernize CVE technology to further scale the program and diversify funding streams in collaboration with the public and private sector.

DANGERS OF DISRUPTION

CVE is about standardization. For example, it enables two or more people to refer to a vulnerability and know they are talking about the same thing. This enables researchers, vendors, and IT professionals to respond to cyber incidents quickly, saving both time and money. Thanks to CVE IDs, other governments and agencies can create enriched databases — such as the NVD and EUVD — tailoring the packages and displays to better suit their needs.

Consequently, a disruption to the CVE program risks fragmentation, slowed incident response, and outdated enriched databases.

Since the initial shutdown scare, the world has seen the launch of CVE alternatives such as the Global CVE Allocation System (GCVE). The birth of multiple vulnerability management databases with distinct ID systems is concerning as it sets the cybersecurity community closer to pre-1999. Fragmentation puts critical infrastructure in key sectors at risk and could lead to global supply chain vulnerabilities for vendors and suppliers.

For now, the European Union Agency for Cybersecurity (ENISA) requires vulnerabilities discovered by or reported to European Computer Security Incident Response Teams (CSIRTs) to be assigned CVE IDs. It is still important to note that the EUVD uses an additional internal proprietary numbering system similar to that of the CVE IDs, with a year and designation formatting. While ENISA could possibly move to EUVD IDs replacing CVE IDs this does not seem to be their intent, the idea that it could clearly move vulnerability enumeration to fragmentation has created a lot of attention to an internal numbering system. The cybersecurity community relies on a standardized approach to vulnerability management and the existence of multiple databases with unique IDs threatens collaboration between researchers, vendors, and organizations.

Slowed incident response exposes systems for an increased time period. This increases the risk of cyberattacks and disrupts security tools that rely on CVE IDs, including patch management systems, vulnerability scanners, Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR).

[5] https://www.thecvefoundation.org/

Further, a lapse to CVE would outdate the external catalogs that rely on the CVE List for enrichment. For example, both the NVD and current EUVD rely on standardized CVE IDs as their backbone. If the CVE List's information is not consistently updated, the databases that rely on it will be rendered useless in the long term.

NEED FOR CHANGE

A program with 25 years of history inevitably faces challenges, critiques, and changes. What unfolded earlier this year has directed increasing attention to the future of CVE, leading researchers, vendors, organizations, and governments to envision and develop alternatives to the current CVE as a way to seek stability in vulnerability management and continue to increase automation in cybersecurity. In order to develop the best solutions to CVE, we first must have general agreement on the main areas for discussion and questions that need to be answered.

Lacking Investment

The current lack of investment in the CVE program has led to operational inefficiencies and a lack of innovation. Technical investments — such as in scalable APIs, machine-readable formats, and automation tools — can modernize infrastructure, empowering CVE to get ahead of emerging vulnerabilities. Reducing manual workflows can create more efficient processes that scale with demand.

Threat of Balkanization

With everyone's best interest at heart, balkanizing vulnerability management is perhaps the most concerning. This is not to say that enrichment is bad but rather that enriched databases should not separate their identifiers from the existing standardized CVE IDs. A globally accepted CVE is key, and ideally any modifications made would be to the one with 25 years of history.

Single-Nation Ownership

The U.S. government's contract blip with MITRE highlighted the challenge of CVE having a sole funder. The question in conversation should go beyond who and what is funding CVE and ask where the funding is going. Diverse and international funding streams prevent CVE from experiencing potential funding-related disruptions while encouraging international collaboration and allowing it to grow with evolving technologies and threats.

Governance is a key topic of conversation and it is important that CVE is viewed as a global collaboration. There is no statutory language marking CVE as a U.S. possession. The program has worked for years under DHS sponsorship. However, it should never give the feeling that CISA alone has an unbounded authority over CVE's structure and future.

Therefore, CISA taking more of an ownership role may be harmful, ENISA's creation of the EUVD was largely due to the EU's impression that CVE was becoming more of a U.S. program rather than a global program. Their decision to create a possible safety net from CVE dependence shows that while the current widespread use of CVE continues and it is clearly conveyed as a public and global good, worries do exist.

Structural Governance

Discussions on CVE modifications should also highlight the program's organizational hierarchy. Before the implementation of Top-Level Roots and Roots, all CVE information was written and published by MITRE. However, even with the existence of Top-Level Roots and its hierarchy of Roots and CNAs, CVE information is still heavily concentrated in MITRE and CISA. Creating a bottleneck restricts CVE from its full responsibility to serve the global community.

LACKING TRANSPARENCY

Funding transparency is also important to prevent power abuses and to understand how money is being spent. As of now, we know that DHS has contracted MITRE by outlying $13.2 million and committing $24.2 million, with a potential award amount of $57.8 million.[6] This funding contract supports several other programs besides CVE, including ATT&CK and Common Weakness Enumeration (CWE). How much of this funding is going directly to CVE — and to support what specifically — is unknown to its users.

This transitions into the importance of a user-first approach. CVE needs to be reactive to the industry based on its users' needs. As Board members, researchers, and industry experts brainstorm ideas to improve upon CVE, there are a few questions that should remain at the forefront of every conversation:

- How can CVE diversify its funding streams while balancing influencers' comments and prioritizing serving the public?
- How can CVE reunite the global cybersecurity community to ensure that everyone is working together toward a common goal?

[6] https://www.usaspending.gov/award/CONT_AWD_70RCSJ24FR0000018_7001_70RSAT20D00000001_7001

AREAS FOR EXPLORATION

There are many ideas on how to go about collaborating and funding the program to progress. Some questions for the global stakeholder community to consider include:

- What combination of funding works best?
    - **Government funding** - This includes U.S. government agencies besides CISA, in addition to international governments. How do we continue to ensure the use of the CVE ID as the global identifier?
    - **Nonprofit funding** - There's the possibility that nonprofits with large endowments could support the CVE, still, questions around spending restrictions and funding sustainability would need to be addressed.
    - **Private sector** - Vendors worldwide use CVE as the standardized form of vulnerability management, so the private sector should be considered as a funding source. Questions around vendor funding to gain leverage in modifying the CVE priority agenda would need to be addressed.
    - **Individual funding** - Likely the least sustainable option, but it is still a stream to consider. CVE would need to prioritize program needs over funder priorities.
- Could international governments that are already CNAs, expand the program further and foster global cooperation? During a time when the EU is seeking technological sovereignty, seeking funding from international governments and bringing them into CVE's governance would make CVE less of a U.S.-focused tool, and more of a global good.
- What's the best CVE structure?
    - Who should hold the majority of CVE authority while maintaining inclusivity and neutrality?
    - What should the organizational hierarchy look like?
    - A more federated system under the governance of a non-governmental organization?
    - A collaborative funding model between additional U.S. government agencies and international governments?

NEXT STEPS

MITRE's contract with CISA expires on March 16, 2026. Within the next year, it is expected that different people and organizations will come forward with suggested answers to the questions raised above.

Whatever the ideas to modernize CVE look like, it is imperative that we work as one. Reforming vulnerability management is not a race to the finish line. With too many disparate databases, CVE's 25 years of standardization and service as a global good will be lost.