CISA Strategic Focus

CVE Quality for a Cyber Secure Future

Overview

Over the past decade, the Common Vulnerabilities and Exposures (CVE) Program has established itself as the global standard for vulnerability identification. This period represents the CVE Program's *Growth Era*, characterized by the successful recruitment of an extensive worldwide network of more than 460 CVE Numbering Authorities (CNAs). This network has contributed to exponential growth in the cybersecurity community's capacity to identify, define, and catalog hundreds of thousands of vulnerabilities. As the CVE Program evolves to meet the needs of this global cybersecurity community, it must transition into a new era focused above all on trust, responsiveness, and vulnerability data quality.

Energizing the CVE Program's *Quality Era*

At the Cybersecurity and Infrastructure Security Agency (CISA), we believe the CVE Program stands as one of the world's most enduring and trusted cybersecurity public goods. It must be led with commitment to conflict-free and vendor-neutral stewardship, broad multi-sector engagement, transparent processes, and accountable leadership. National security and public safety require government accountability, as demonstrated in other critical safety areas like automobiles, aviation, pharmaceuticals, and medical devices, to name a few. Software vulnerabilities require a similar level of accountability, given the ubiquity of software that underpins critical infrastructure systems.

Privatizing the CVE Program would dilute its value as a public good. The incentive structure in the software industry creates tension for private industry, who often face a difficult choice: promote transparency to downstream users through vulnerability disclosure or minimize the disclosure of vulnerabilities to avoid potential economic or reputational harm. These built-in conflicts could have a detrimental impact on program transparency and the ability to continue standardizing disclosure practices through the public identification and cataloging of vulnerabilities. In addition, although alternative stewardship models might seem appealing, they can lack stability and become vulnerable to undue financial pressures or contribution-driven influence. These conflicts of interest reinforce the need for CISA to take a more active role in the long-term stewardship of the CVE Program. At CISA, we have the appropriate mandate, relationships, and capability as the U.S. federal agency that leads public/private partnership programs, global coordinated vulnerability response, and are explicitly responsible for protecting the nation's critical infrastructure from cyber threats.

Moving forward, CISA believes it is critical that the CVE Program maintain a core principle: CVE data must remain free and openly accessible as a public good. This principle underpins coordinated cyber defense, enables innovation in security tooling, and empowers defenders across industry and government worldwide. CVE Program stewardship must reflect this and be managed as a public good with global participation in its governance.

As we collaboratively work through a detailed roadmap, we want to provide our perspective on CVE's future priorities. These priorities are informed by our role in the CVE Program, as well as feedback received from the broader community.

Partnerships Matter

The dialogue over the past several months has opened the door to new relationships, conversations, and valuable feedback about the CVE Program. Thank you to our community members for engaging with us and for all that you do to make the program a success. Your support for open source products, integrations, participation as a CNA, feedback on Vulnrichment, optimizations to vulnerability prioritization frameworks, and working group efforts is essential. CVE would not be what is today without you!

As we look to the future of the CVE Program, CISA is committed to working hand-in-glove with the community to ensure we strengthen and improve the CVE Program.

If you would like to provide feedback on our vision and lines of effort or simply aren't currently part of the CVE Program and have interest in contributing, please email us at Vulnerability@cisa.dhs.gov.

CVE Quality Era Lines of Effort

Expand on Community Partnerships: The CVE Program advisory board should be a holistic representation of the ecosystem. CISA intends to leverage its partnerships to ensure better representation from international organizations and governments, academia, vulnerability tool providers, data consumers, security researchers, the operational technology industry, and the open-source community. A more diversified and international program will yield valuable insights and innovations.

Government Sponsorship: As a critical public good, the CVE Program's infrastructure and core services require ongoing investment from CISA. Many in the community have requested that CISA consider alternative funding sources. As CISA evaluates potential mechanisms for diversified funding, we will update the community.

Modernization: CVE infrastructure modernization and value-added services development must accelerate to meet the needs of a scaled, operational, and global program. CISA intends to prioritize more rapid implementation of automation and other capabilities, specifically improving CNA services, expanding API support to downstream data consumers, and improving CVE.org.

Transparency and Communication: Transparency is central to trust. CISA is committed to seeking community feedback and incorporating it into program roadmap decisions, regularly communicating program milestones and performance metrics, and actively engaging in dialogue with global partners.

Data Quality Improvements: CISA has been tracking the completeness trends of CNAs contributing to the program. In August 2025, 79.9% of all CNAs that published a CVE Record in the previous six months included CVSS and CWE information in their publication, a 9.4 percentage point increase from a year earlier. This is a significant step in achieving a higher standard of minimums and modernizing approaches to improve CVE Record quality. CISA is committed to partnering with industry and international governments to implement new minimum standards for CVE Record quality and develop federated mechanisms to scale enrichment, such as Vulnrichment and the Authorized Data Publisher (ADP) capability. We look forward to working with the community to find creative ways to achieve quality, improve the CVE schema, and forge ahead with innovative solutions that bring automation, machine learning, and artificial intelligence into the portfolio.

Improvements in CNA of Last Resort (LR): Improving transparency, visibility, responsiveness, and data enrichment across all CVE Records is important for the CVE Program to fulfill its mission. While promoting CVE Program federation in the form of CNA community growth, CISA will also prioritize improvements in these areas appropriate to the unique roles that CNA-LRs play in the ecosystem. CISA will lead by example and manage program performance by raising the standards for transparency, communication, and responsiveness to community queries.