



25th Anniversary Report

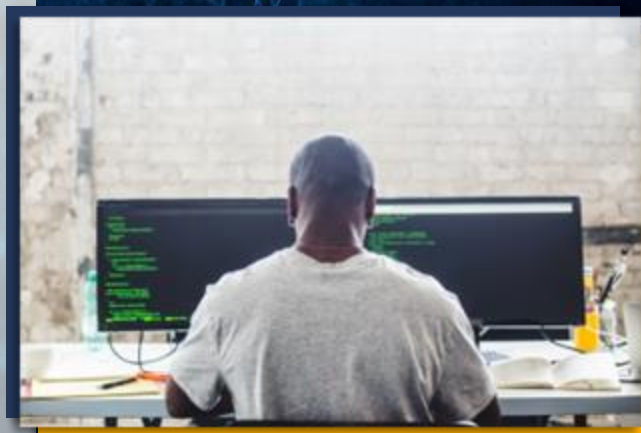
October 2024

CVE™ is 25!

Over the past 25 years, the CVE Program has been established as the de-facto international standard for vulnerability identification and the backbone of the vulnerability management ecosystem.

Now with over 400 CVE Numbering Authority (CNA) program partners spanning 40 countries, the CVE Program continues to evolve and grow while remaining true to its enduring mission: to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

We invite you to explore this report to reflect on past achievements and look forward to new challenges and opportunities to continue modernizing and evolving the CVE Program into the next 25 years.



Introduction

Founders Corner 3

CVE Program Sponsors 4

CVE Program Origins

CVE Program Origins 5

Mission, Goals, and Value Proposition 7

Initial Growth, Scaling Challenges 8

Modernizing through Federation

Reinvigorating the Board 10

New Operational Model, New Roles 11

Program Growth through Federation 12

Enabling Federation 13

The CVE Program at 25

Program Structure 19

Downstream Data Consumers 20

Events in the Community 21

Outreach and Communications 22

New Challenges & Opportunities

Evolving Community Engagement 25

Increasing CVE Record Value 26

Diversifying the CNA Community 27

Common Identifier for Prioritization 31

Program Metrics Overview

Year over Year Metrics Review 33

Founder's Corner

— Ken Armstrong, Ken Williams,
Kent Landfield, and Scott Lawler —



Whether personal or professional, anniversaries are an opportunity to reflect on progress and inspire ideas for the future. The Common Vulnerabilities and Exposures (CVE) Program turned 25 years old in 2024. As the four, still active original founders of CVE, when we reminisce on its progress since 1999, it provokes feelings of nostalgia.

Over its history, the program transformed from a modest passion project to a global cornerstone for identifying and enabling defenders to address vulnerabilities. In 2016, the CVE Program had just 24 CVE Numbering Authorities (CNAs). Today, that number has surged to over 400 and is growing weekly. The expansion of CNAs has broadened the geographical scope of the CVE Program. What began as a United States-centric initiative has expanded to 40 countries participating in the CVE Program. This global collaboration informs a more comprehensive understanding of regional vulnerabilities and threat actor activity. This allows organizations to holistically analyze, track, and mitigate threats locally.

As the program has grown, so have its capabilities. Automation has transformed the abilities for CNAs to rapidly assign, update, and distribute CVEs for identified vulnerabilities, boosting vulnerability mitigations. CNAs are now able to provide enriched detail to CVE Records. While the program continues to evolve and adapt, there are still areas for improvement.

One of these areas is the CVE Program's relationships with the open-source community. CVE has a lingering reputational issue from its earlier days of dense backlogs and long wait times. While those conditions no longer exist, some open-source community members still harbor a grudge. As big names like the Apache Software Foundation and the Python Software Foundation embrace CVE reporting, stronger relationships with the open-source community are building.

To drive even broader acceptance, CVE leaders are pursuing stronger collaboration and incorporating open-source projects as CNAs. The scale and complexity of open-source projects require the automation the program is deploying. Additionally, CVE leadership comes from many differing areas including the open-source community. This has enriched the CVE Program's decision-making process while helping the program better understand the nuance and evolving needs of the community.

Another area for improvement is the need to reframe the stigma of a vulnerability, which leads to a lack of organizational vulnerability transparency. There are still organizations reluctant to disclose vulnerabilities promptly, fearing backlash from customers and stakeholders. This fear stems from an outdated and inaccurate understanding and frames vulnerabilities as an inherent display of weakness.

It is widely understood that all software has vulnerabilities. Companies that openly identify, address and fix vulnerabilities (instead of letting them fester in silence) establish trust with their customers and the industry. Organizations should embrace CVE and understand that acknowledging and resolving vulnerabilities indicates progress, maturity, and a willingness to protect their customers, not a weakness.

Amidst these complexities, there is a new elephant in the room — evolving artificial intelligence (AI). CVE leadership is discussing AI and its ongoing impact on the software industry. The CVE Program must navigate this terrain with caution. AI technology brings forth an entirely new set of challenges. AI-coded vulnerabilities are not like your standard buffer overflow; they add a new dimension of complexity. As AI permeates the actions of SecOps teams and malicious actors, the CVE Program must evaluate the vulnerabilities AI brings to the table and integrate a new approach to proactively address them.

From a policy perspective, continued education of policymakers is critical to the future of CVE. When policymakers understand the importance of the CVE process, we see strong legislative strides (such as CVE specified in the EU's NIS 2 Directive). From integrating with established global vulnerability reporting practices to incentivizing transparency, CVE-aware global governments can play an important role in evolving the vulnerability reporting process.



Reflecting on a quarter century of progress — forged through tough conversations, passionate leaders, and a commitment to a more cyber-secure future — we all are reminded of how far the CVE effort has come. Looking forward, we know the CVE Program will continue to be a valuable cornerstone to help the vulnerability management community step up and meet the global digital ecosystem's rapidly evolving needs.

From the four active, original CVE Board members to the entire CVE community, ***thank you!***

CVE Program Sponsors

- CVE began as a research project at the MITRE Corporation, a non-profit organization that operates Federally Funded Research and Development Centers (FFRDCs)
- In the early years, CVE was sponsored by several different organizations in a multi-agency funding model
 - + The dedication and financial support from many initial champions helped CVE grow and develop into a robust, operational program
- Since the United States Department of Homeland Security's (DHS) establishment in 2003, the CVE Program has been sponsored by various program offices in DHS. Today, CVE is sponsored by the DHS Cybersecurity and Infrastructure Security Agency (CISA).
- CISA is a committed leader in the CVE Program's community of international stakeholders, working to reduce the prevalence and impact of vulnerabilities and exploitable conditions across enterprises and technologies.



PROGRAM ORIGINS

PROGRAM ORIGINS

In 1999:

- Candidate vulnerabilities were voted on by the CVE Editorial Board prior to being included
- 321 CVE Records produced
- MITRE produced all CVE Record descriptions as the only CVE Numbering Authority (CNA)
- US-Centric
- No community working groups

In 1999, there was no common naming convention and no common enumeration of vulnerabilities that existed in disparate databases. As a result, it was labor intensive to compare output from different vendors' assessment or intrusion detection tools (IDS), relate IDS alarms with network assessment probes, and relate any tool with other information sources.

As originally envisioned by Steve Christey Coley and David Mann in *Towards a Common Enumeration of Vulnerabilities*¹, CVE was established to “help to foster easier data sharing.” Thus, CVE’s mission was established to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

CVE Program Mission:

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities

¹ Mann, D., & Christey, S. (1999, January 8). Towards a Common Enumeration of Vulnerabilities. Retrieved from CVE: <https://www.cve.org/Resources/General/Towards-a-Common-Enumeration-of-Vulnerabilities.pdf>

Mission, Goals, Outcomes, and Value

Based on its mission to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities, the CVE Program set two primary goals:

- Goal 1: Increase program adoption

- Goal 2: Increase program coverage

These goals were set to drive CVE usage throughout the vulnerability management ecosystem and enable more vulnerabilities to receive CVE IDs and associated CVE Records, so that organizations can use them to strengthen their vulnerability management programs.

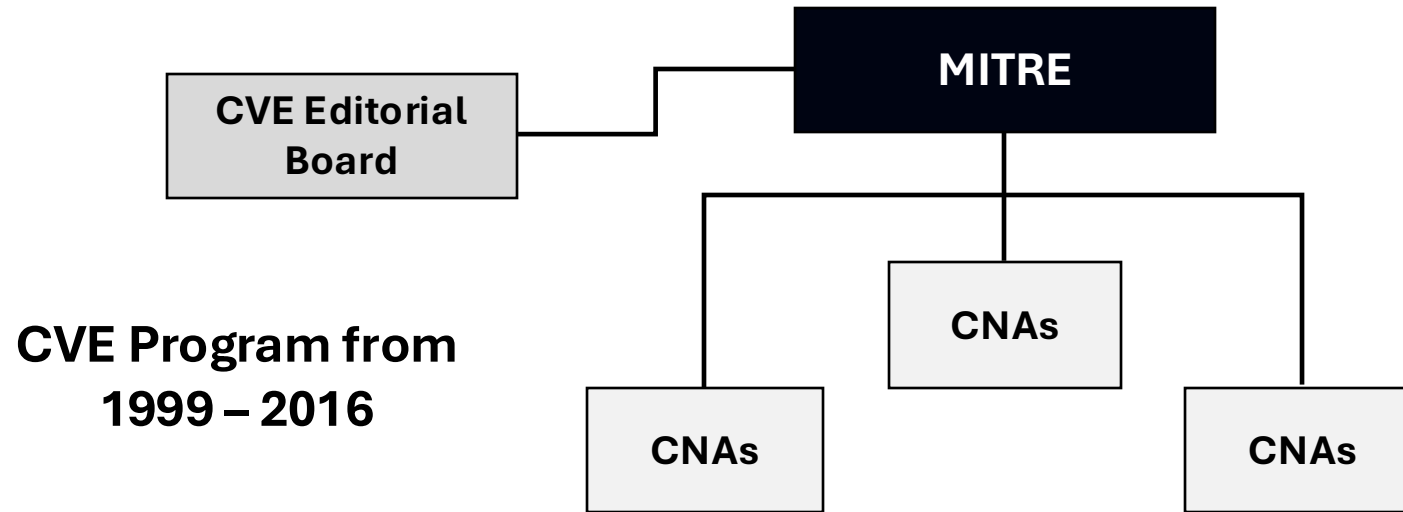
Ultimately, the desired outcome is that more quality CVE Records would be produced more rapidly.

These foundational elements remain the backbone of the CVE Program.



Value Statement

CVE enables two or more people or tools to refer to a vulnerability and know they are talking about the same thing, resulting in significant time and cost savings.



In the beginning, the CVE Program operated in a centralized model where MITRE assigned virtually all CVE IDs across all software products after review by an Editorial Board of representatives from tool vendors, MITRE, academia, and the security industry. CNAs had little agency. A few published advisories that MITRE used to create CVE Records, but communication between them and the CVE Program was minimal.

As businesses started using more and more software, and vulnerabilities started proliferating at a rapid pace, CVE's hub-and-spoke model began to struggle under the demand. This model was not scalable to meet the challenges of the new vulnerability landscape.

CVE was at a crossroads.

Initial Growth and Scaling Challenges



**MODERNIZING
THROUGH
FEDERATION**

The CVE Editorial Board became the CVE Board, which is responsible for the strategic direction, governance, operational structure, policies, and rules of the CVE Program.

In 2016, the CVE Board, which included CISA sponsors, other government and industry, and MITRE, began meeting every two weeks, with the goal of federating CVE Program governance and operations as its top priority. Core to the new strategy was the principle that no single organization could handle the entire assignment, record publication, and governance workload.

Moreover, the existing program infrastructure, from automation to rules and policies, required enhancements for the challenge at hand.



Modernizing the Program

- Reinvigorating the CVE Board
- Developing a strategy to scale
- Expanding existing roles and creating new roles
- Recruiting and onboarding more partner organizations
- Creating an infrastructure to support federated governance and operations
- Working with community partners to do the difficult work required to right the program

Charting a New Path

New Operational Model, New Roles

In October 2016, CVE adopted a federated model which required CNAs to publish their own CVE Records consistent with the newly published CNA Rules. These rules required CNAs to publish their own CVE Records within their scope.

This had the desired effect of pushing CVE ID assignment and record publication to those with the most knowledge of the vulnerabilities – those closest to the products – while concurrently distributing the workload so that the program could scale.

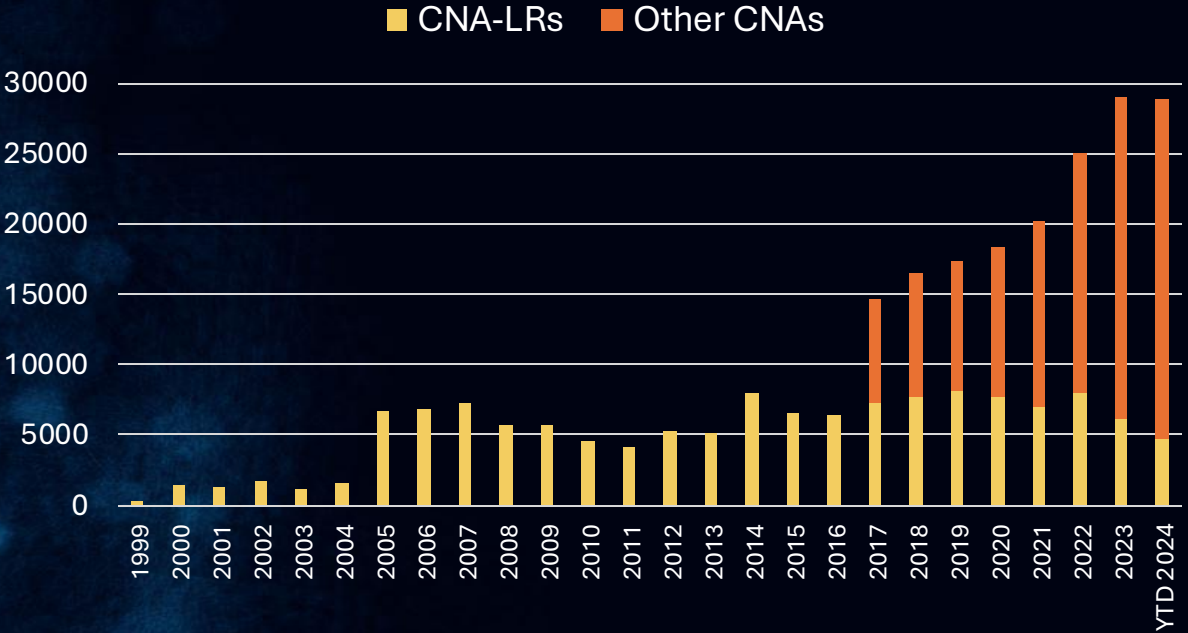
This approach incentivized more organizations to become CNAs and control the CVE publication release process for vulnerabilities in their scope. CNA recruitment and onboarding rapidly accelerated. The total number of CNAs increased by over 700% from 45 in 2016 to over 400 in 2024.

As the number of CNAs increased, a single organization could not govern them all given language barriers, realms of technical expertise (e.g., ICS/OT), and other considerations. Thus, the Board created two new roles:

- **Roots:** An organization authorized within the CVE Program that is responsible, within a specific Scope, for the recruitment, training, and governance of one or more entities that are a CNA, CNA of Last Resort (CNA-LR), or another Root
- **Top-Level Roots (TLR):** A Root that is responsible for the governance and administration of its hierarchy, including Roots, CNAs, and CNA-LRs within that hierarchy

A **CNA of Last Resort** (CNA-LR) is authorized to assign CVE IDs and to publish CVE Records within a TLR or Root's scope for vulnerabilities that are not covered by the scope of another CNA. Thus, any vulnerability meeting the CVE Program's rules will receive a CVE ID and CVE Record for the benefit of the community using publicly available information.

Year	Records Published	Number of CNAs	% of Total Production: Volunteer CNAs	% of Total Production: CNA-LRs
2016	6,457	24 (5 Int.)	0%	100%
2017	14,644	78 (22 Int.)	50%	50%
2018	16,510	90 (26 Int.)	53%	47%
2019	17,308	106 (37 Int.)	53%	47%
2020	18,364	144 (61 Int.)	58%	42%
2021	20,161	209 (100 Int.)	65%	35%
2022	25,059	263 (126 Int.)	68%	32%
2023	28,961	354 (165 Int.)	79%	21%
9/30/24 (YTD)	28,392	408 (189 Int.)	84%	16%



CVE Record production scaled rapidly with the program’s federation between 2016–2017. Not only were more records being produced, the burden on the CNA-LR was lessened with each CNA that was added to the program.

CVE Program Growth through Federation

Enabling Federation: Community Engagement

Strategic Planning Working Group

Automation Working Group

Quality Working Group

Community of Peers (formerly CNA Community Working Group)

Outreach and Communications Working Group

Tactical Working Group

Vul. Conference & Events WG

AI Working Group

**Beyond CNAs,
federating the CVE
Program also required
engaging its stakeholder
community through working
groups to help drive its supporting
strategic, operational, and coordination activities.**

2017

2018

2019

2020

2021

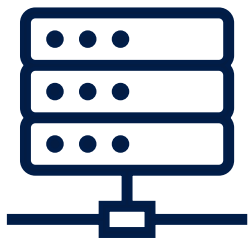
2022

2023

2024

2025

Enabling Federation: Automation



The CVE Program needed automation to:

- Support program governance and operations in a federated environment
- Improve CVE ID reservation and CVE Record publication by removing manual intervention

Automating data exchange was a top priority to enable CVE Program federation as it meant the ability for more distributed activity throughout the growing CVE community. Initial planning began in late 2016 with tangible infrastructure planning and services descriptions occurring through 2017 and 2018.

Community partners were essential in designing, developing, and implementing CVE automation services including the CVE Identification Reservation (IDR) system and the Record Submission and Upload service (RSUS). IDR enables CNAs to reserve only the required number of CVE IDs at a given point in time and moved the program away from block ID requests. RSUS and the new CVE Record format enable CNAs to submit records directly to the CVE List, bypassing manual review by the CVE Program Secretariat.

“

I used to send MITRE a spreadsheet with information about the new Patch Tuesday CVEs when I remembered to do it.

Now it is just part of the job to update the Security Update Guide publishing process.

Even as a CNA, it used to take days or weeks to reserve a CVE ID. Now it takes seconds! ”

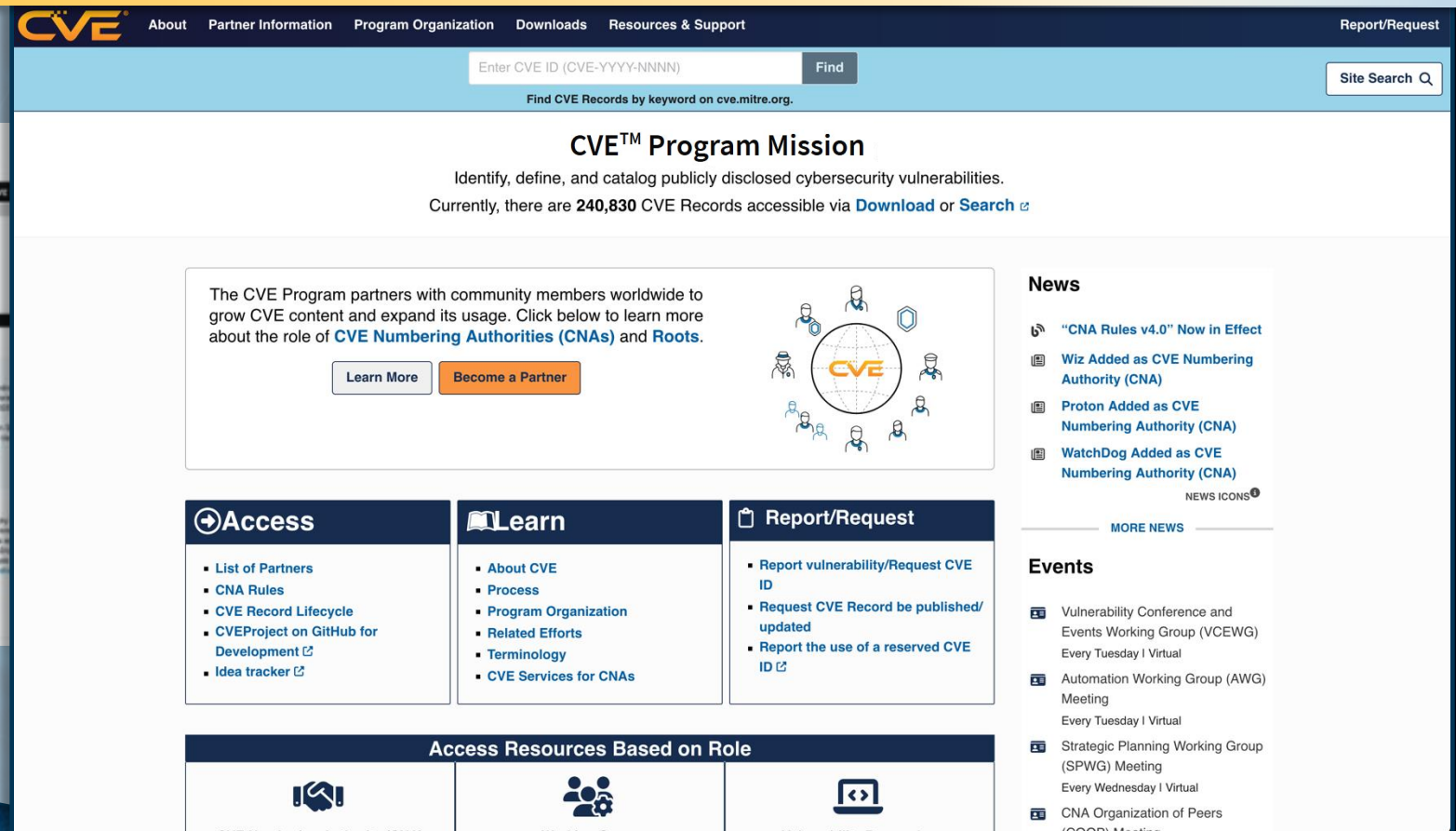


Lisa Olson

Principal Security Program Manager
Microsoft
CVE Board Member

Enabling Federation: Communication

from  ...



In October 2021, the CVE Program launched a new website under the cve.org domain with greater usability and improved information resources for the vulnerability management community.

... to 

“

The New CVE Record Format is a more complete data structure that supports a variety of valuable data elements. Now that CNAs are putting more enriched data in the new record format, I can do my research all on cve.org.”



Art Manion
Deputy Director
Analygence Labs
CVE Board Member

In 1999, a CVE Record consisted of only three elements: the CVE ID, a brief description, and an external reference directing to further relevant information about the vulnerability. The CVE List could be viewed on the MITRE website directly or downloaded in its entirety in a variety of formats.

As businesses used more software and vulnerabilities proliferated, the CVE Program needed to expand its ID syntax from supporting more than a maximum of 9,999 unique identifiers per year (CVE-YYYY-NNNN). The change to support an ID of indeterminate length impacted a variety of products, tools, websites, and processes that needed to update.

In 2018, the CVE Program introduced CVE JSON 4.0, which allowed specific data such as vendors, products, versions, vulnerability types, and impacts to be captured in their own separate fields. Working groups and test pilot programs ensured all relevant vulnerability data could be included and easily consumed by downstream users.

Then in 2022, CVE JSON 5.0 – renamed the CVE Record Format – added several new features and improvements that further enabled CVE data consumption through increased standardization and machine-readability. CVE Record creation and publication could now be automated, meaning more quality CVE Records could be produced at a faster pace.



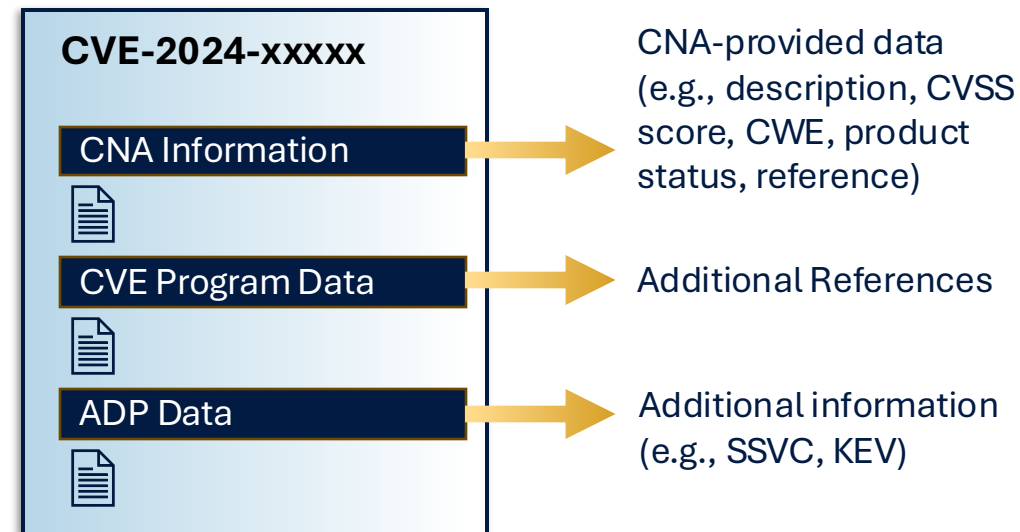
The CVE Record Format

Over the last 25 years, the CVE Record Format evolved from an unstructured set of only three data elements to a rich, structured format capable of handling a large variety of data elements as needed for vulnerability management.

The CVE Quality Working Group meets bi-weekly to find ways to improve the CVE Record Format and make it more accessible and useful across a wider audience both within and outside of the security community.

Enabling Federation: CVE Record Format

While most CVE data is produced by CNAs, 2024 introduced a new CVE data provider – the Authorized Data Publisher (ADP). An ADP is an entity authorized to enrich the content of CVE Records published by CNAs with additional, related information (e.g., risk scores, references, translations). The intent is to enhance the value of a CVE Record by providing the community with further valuable information from an authorized entity.



Consistent with the CVE Record Format:

- ADPs have their own specific container in which they enrich CVE Records with added information within their authorized scope
- An ADP cannot modify the data the CNA has in their “CNA container”

In June 2024, the CVE Program operationalized the first ADP, run by CISA. It is authorized to provide several components to enrich CVE Records:

- Stakeholder-Specific Vulnerability Categorization (SSVC)
- Known Exploited Vulnerabilities (KEV) Catalog data
- “Vulnrichment” Updates including CVSS, CWE, and CPE information for CVE Records (when not provided by the CNA) that meet specific threat characteristics

Enabling Federation: Data Enrichment



THE CVE PROGRAM AT 25

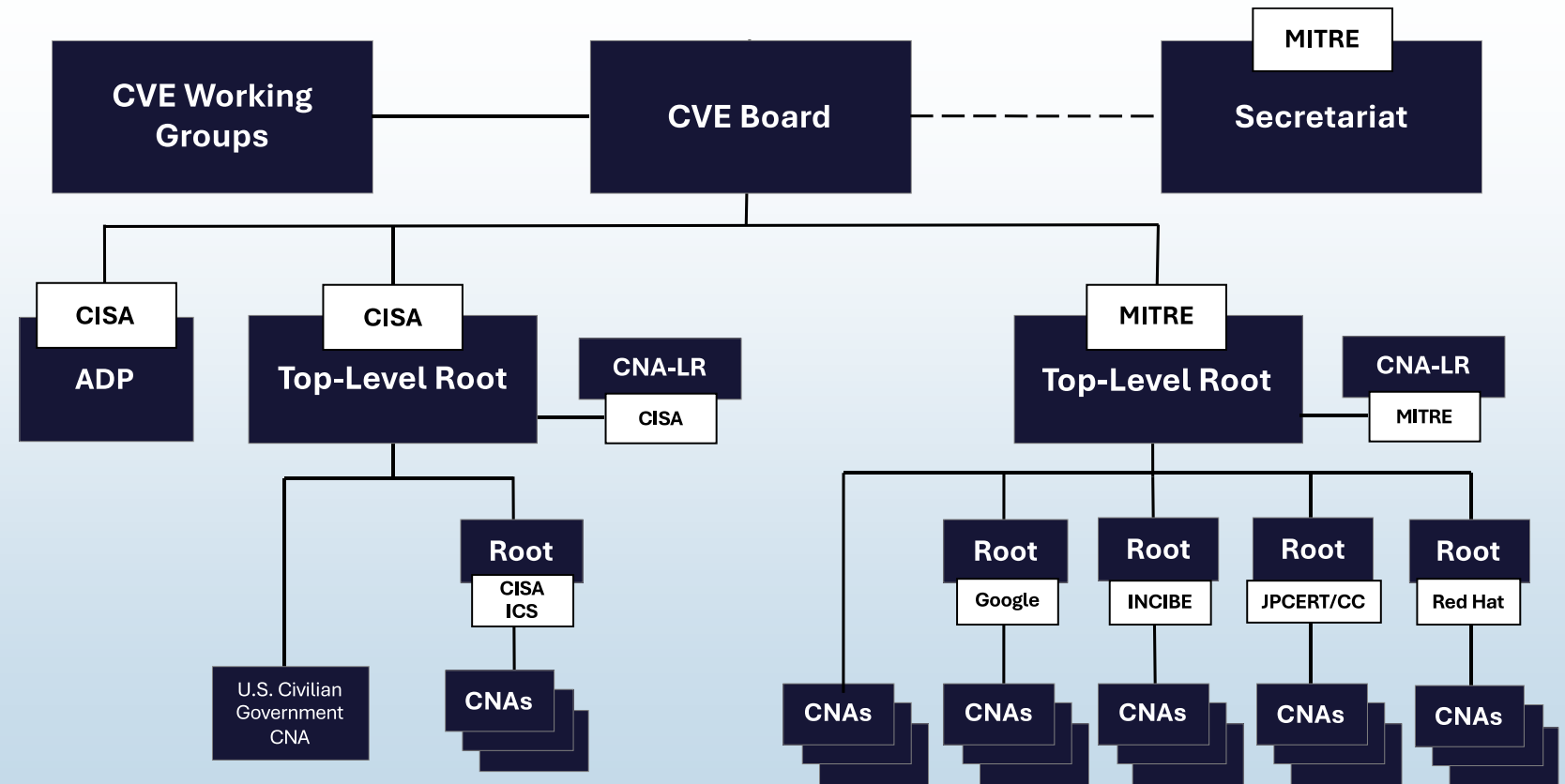
CVE at 25: Program Structure



Federation in Action:

- + 8 Working Groups
- + 2 Top-Level Roots
- + 5 Roots
- + 2 CNA-LRs
- + 408 CNAs
- + 2 ADPs
- + 40 Countries

metrics as of 9/30/2024



CVE at 25: Backbone of the Vulnerability Management Ecosystem

CVE Records Feed a Multitude of Downstream Data Consumers Across Industry, Government, and Academia

National Databases and Advisories

*Identify and track security
vulnerabilities*

NVD

National Vulnerability Database

National Cyber Security Centre – NL

 Canadian Centre for Cyber Security

ACSC Australian Cyber Security Centre

and more...

Tool Vendors

*Communicate vulnerability
advisories to customers*

Vulnerability Management

Security Information and
Event Management (SIEM)

Endpoint Protection Platforms

Patch Management Tools

Webapp / Network / Cloud /
Container Security Tools

and more...

Incident Response Operations

*Identify vulnerabilities, assess severity,
analyze root cause, and case manage*

CSIRT

Computer Security Incident
Response Teams

PSIRT

Product Security Incident
Response Teams

**National Cyber
Incident Response**

Data Scientists, Researchers, Policy Makers

*Identify trends and the evolving
landscape of threats, affect change*

Vulnerability Intelligence
Platforms

Academia



CISA BOD 22-01
Known Exploited Vulnerabilities



CVE at 25: Events in the Community

CVE hosts several community events throughout the year including technical workshops and webinars for CNAs and downstream data consumers, as well as the annual VulnCon conference together with FIRST.

The 2024 CVE/FIRST VulnCon was the inaugural vulnerability-focused conference, a milestone culminating CVE's growth as an international, community partnership program.

The 2025 CVE/FIRST VulnCon promises an exciting docket of dynamic speakers and cross-industry topics to accelerate collaboration across the vulnerability management and standards / frameworks communities.

40+ sessions across 3 days of content, networking, and collaboration

Vulnerability metadata SIGs, Working Groups, and other experts

Speakers from global CERT teams, OpenSSF, ENISA, FIRST, CISA, MITRE, and others

Detailed sessions on frameworks like CVE, CWE, CVSS, EPSS, KEV, VEX, CVD, and SBOM

The CVE Program engages the community on *multiple channels* to:

- + Share data
- + Provide program updates
- + Recruit new program partners
- + Build awareness



All Subscribers
114,000+ signups



CVE Videos
101,000+ views



CVE Podcast
33,000+ listens



CVE Blog
24,000+ views

Feeds

New CVE Records

[X-Twitter](#) [cvelistV5 repository on GitHub](#)

CVE Program News

[CVE Website](#) [X-Twitter](#) [LinkedIn](#) [Mastodon](#) [Email Newsletter](#)

“We Speak CVE” Podcast

[YouTube](#) [Buzzsprout](#)

Videos

[YouTube](#)

Blogs

[CVE Website](#) [Medium](#)

CVE at 25: Outreach and Communications



**NEW CHALLENGES
AND OPPORTUNITIES**

Taking CVE Forward Into the *Next* 25 Years

- **Evolving Community Engagement**
- **New Challenges and Opportunities**
 - + Increasing the Value of CVE Records
 - + Broadening the organizational diversity within the CNA Community
 - + Strengthening the connection between CVE Program and downstream data consumers
 - + Providing a foundation for new cybersecurity solutions / defenses

The CVE Program's federation strategy has scaled the program and made it the de-facto standard for vulnerability identification.

A thriving international partnership community and mature program governance structure continues to further drive its goals to increase program adoption and coverage.

But there is still much to do as *CVE looks forward...*

Evolving community engagement means *direct and collaborative* opportunities for:

- The CVE Program to continue learning from vulnerability management practitioners on what is needed to advance the state of practice and improve CVE Program services and operations
- Downstream CVE Program users and participants to better understand program developments and learn CVE best practices

CVE will continue to modernize through direct engagement with its diverse community of stakeholders across its many working groups.

Periodic collaborative workshops with CNA partners and downstream consumers will continue to help answer questions and find ways to improve CVE.

If you'd like to join a working group, visit cve.org

“

The CVE Program learns from the vulnerability management community, evolving through shared expertise and collaboration.

By listening to those who actively manage and disclose vulnerabilities, CVE continually advances to better serve the global security ecosystem.”



Katie Noble
Director, PSIRT and Bug Bounty
Intel Corporation
CVE Board Member

CVE Looking Forward: Community Engagement

As the CVE data format evolved to support additional fields, additional vulnerability-related information has become important to the cybersecurity community for increased transparency, vulnerability root cause understanding, and prioritizing incident response. These include CVSS, CWE™, CPE, and others.

Incorporating additional data elements of value directly into the CVE Record means greater benefit for defenders and downstream customers on a timelier basis. The CVE Record can be the “one-stop-shop” for vulnerability information.

STATISTICS (2024)	Apr 2024	Oct 2024	Increase
Total number of CNAs	368	411	+ 43
CNAs assigning CVSS	222	253	+ 31
CNAs assigning CWE	202	236	+ 34
CNAs assigning CVSS + CWE	184	214	+ 30



In April 2024, the CVE Program launched an initiative to encourage CNAs to enrich their CVE Records with additional valuable data elements at the time of disclosure. As the authoritative source of vulnerability information (within their CNA scope), and with access to the most reliable sources, CNAs are the best positioned to make accurate scoring and mapping determinations.

The table on the left illustrates how CVE Program partners around the world are quickly adopting data enrichment as part of their vulnerability disclosure process. The CVE Program recognizes them by publishing the biweekly CNA Enrichment Recognition List (ERL) on cve.org. Within six months of the CVE Program launching the enrichment initiative, the ERL had 221 CNAs on it, representing 54% of the total CNA community.

As additional data elements are identified that further increase the value of the CVE Record for downstream consumers, the CVE Record, and the ERL criteria, may continue to evolve.

CVE Looking Forward: Increasing the Value of the CVE Record

CVE Looking Forward: Diversifying the CNA Community

Since the CVE Program began in 1999, the role of cybersecurity in industry, commerce, and government has grown considerably, as has the global cybersecurity community.

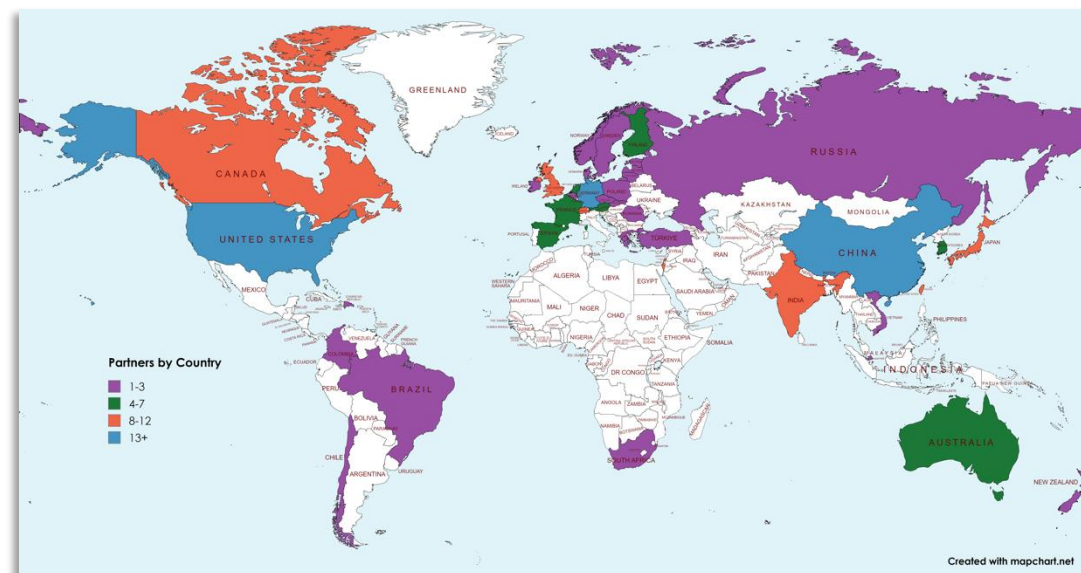
In an evolving global cybersecurity landscape, the CVE Program must continue to:

- Strengthen relationships with *existing* program partners
- Establish *new* relationships with organizations across strategically important but underrepresented domains



Increasing participation of... *Underrepresented Industries in the CNA community*

As it celebrates its 25th anniversary, the CVE Program must continue to expand its community of program partners into currently less represented industries, ensuring vulnerabilities in these domains are properly identified and covered by the CVE Program.



Opportunities for growing CVE Program coverage through onboarding additional CNAs in underrepresented, critical industries include:

- **Automotive**
- **Financial Services and FinTech**
- **IoT and Smart Devices**
- **Critical Infrastructure and Energy**
- **Telecom Providers and ISPs**
- **Healthcare and Pharmaceutical Technology**
- **AI and Machine Learning**
- **E-commerce and Retail**
- **Cloud-native Platforms and SaaS**

Governments and International Community



Governments around the world continue to turn to the CVE Program for vulnerability identification

- The European Network and Information Security Agency (ENISA) became a CNA in January 2024
- The European Union's NIS 2 Directive instructs ENISA to work with the CVE Program

Governments around the world are turning to CVE as the de facto international standard for vulnerability identification. As we welcome this programmatic success, there remains a tremendous opportunity in continuing to build partnerships in the global community across industry, government, and academia.

The CVE Program can continue to engage in active diplomatic outreach and further promote CVE adoption through multilingual and culturally tailored resources. The more CVE can employ legislative advocacy as it did with the NIS 2 Directive, the greater the benefit for the global vulnerability management community.

There are further opportunities for organizing and participating in international workshops and community engagement activities. Encouraging international collaboration in vulnerability disclosure will have the cumulative effect of growing the CVE Program adoption and coverage, as well as expanding the network of international CNAs.

“

Python users around the world rely on accurate vulnerability data to keep themselves and their users safe. The Python Software Foundation becoming a CNA means there will always be up-to-date information on core projects like CPython and pip, as well as PSF staff with expertise on CVE as a resource for the community.”



Seth Larson
Security Developer
Python Software Foundation

More and more software development relies on open source projects and components, and there are some unique challenges to CVE identification in open source.

The CVE Program has been building relationships with many significant OSS community organizations, including:

- Apache Software Foundation
- Canonical
- Debian Project
- Python Software Foundation
- GitHub
- Jenkins Project
- Kernel.org
- Mattermost
- Mozilla
- Node.js
- OpenHarmony
- OpenSSL
- Red Hat
- Suse
- and others...

Challenges:

- Unlike the vendor community, the open-source software (OSS) community often lack resourcing for vulnerability response
- CVE ID assignments in OSS can be inaccurate and include exaggerated severity without input from the maintainer(s) or other SMEs
- It is challenging to determine where in the software supply chain CVEs should be assigned

CVE will *build* on its initial wins and continue to improve CVE adoption and coverage in the OSS community by working *with* them.

Increasing Participation with Open Source

The Foundation for Vulnerability Prioritization

CVE is the pivot point for cybersecurity risk management and prioritization.

Industry and researchers score and prioritize CVE Records using a variety of criteria, including:

- Severity
- Stakeholder context
- Exploitability
- Impact
- and others...



Common Vulnerability
Scoring System



Stakeholder-Specific
Vulnerability Categorization



Known Exploited
Vulnerability Catalog



Common Weakness
Enumeration




Common Security
Advisory Framework

... and others still to come

As the community learns more about adversary behavior and develops *new* methods to prioritize vulnerabilities, CVE will remain the common identifier on which to coordinate



Select CVE Program Annual Metrics



Select Annual Metrics

Year over Year | Q3 2023 – Q3 2024

24.1%

Increase in
CVE Records
published

31.8%

Increase in
CVE Records
published by
Supplier CNAs

47.2%

Increase in
CVE Records
enriched with
CVSS & CWE

15.0%

Increase in
CNAs Added to
CVE Program

46.7%

Increase in CNAs
with 'Hosted Service'
(cloud) in their CNA
scope

147 → 189

Growth in International CNAs

321 → 409

Growth in Total CNAs



In the last 12 months, the CVE Program has had sustained growth in key metrics, including federated CVE Record production as well as federated data enrichment by a growing global community of CNAs.

Q3 2023 to Q3 2024 also saw a large increase in CNAs covering vulnerabilities in software delivered through the cloud. This important metric reflects that the CVE Program remains critical for vulnerability disclosure during the broader trend from on-premise software to cloud-hosted software-as-a-service (SaaS).



thank YOU!

A heartfelt thank you to Steve Christey Coley and David Mann for the original vision and initiative in launching and building CVE into an operational program.

The CVE Program's continued growth and success over its 25-year history are due to the hundreds of organizations and thousands of individuals who have devoted their time and effort to its development and ongoing achievements.

We look forward to the ongoing collaboration with our community partners as we begin the CVE Program's next 25 years!



The mission of the CVE Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by CVE Numbering Authorities (CNAs) from around the world that have partnered with the CVE Program. CNAs publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities.

Learn more www.cve.org



CVE is sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2024, The MITRE Corporation. CVE and the CVE logo are trademarks of The MITRE Corporation.