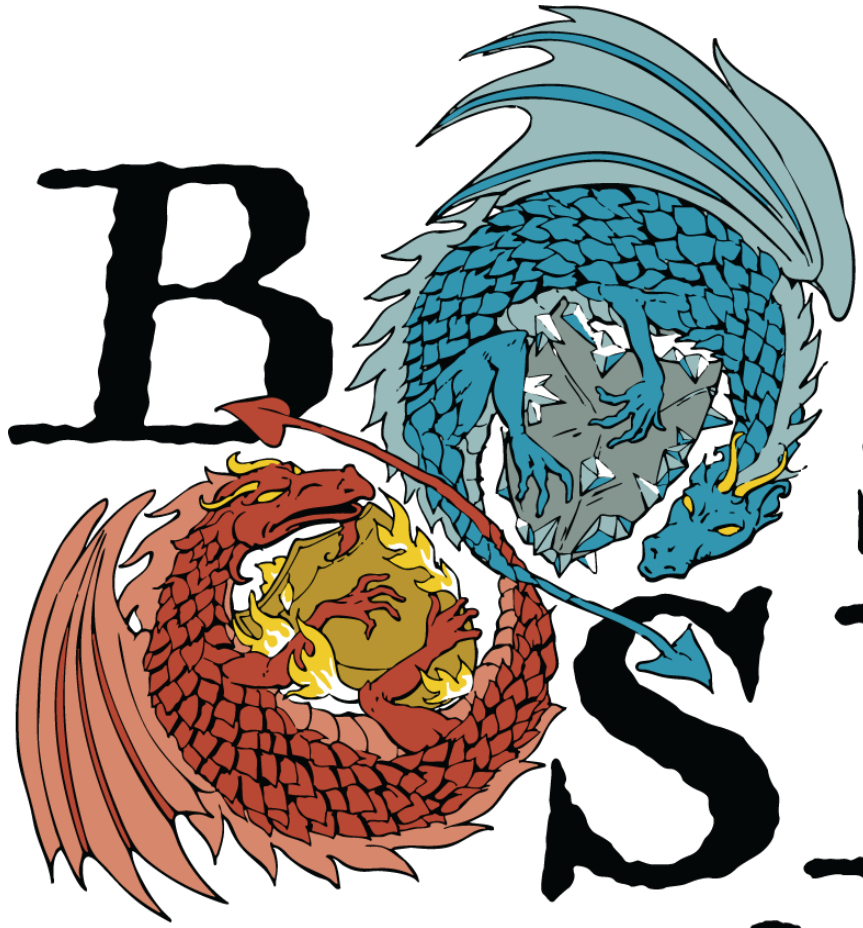


BSIDES San Francisco 2025

The Growing Crisis in CVE Data Quality

BSides San Francisco
April 27th 2025

Q&A
(via Slido)

Feedback
(2 questions)

About Me

Jerry Gamblin

jerry.gamblin@gmail.com

@jgamblin (X/Etc)

jerrygamblin.com

cve.icu

Record Scratch
Freeze Frame

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

April 15, 2025

Dear CVE Board Member,

We want to make you aware of an important potential issue with MITRE's enduring support to CVE.

On Wednesday, April 16, 2025, the current contracting pathway for MITRE to develop, operate, and modernize CVE and several other related programs, such as CWE, will expire. The government continues to make considerable efforts to continue MITRE's role in support of the program.

If a break in service were to occur, we anticipate multiple impacts to CVE, including deterioration of national vulnerability databases and advisories, tool vendors, incident response operations, and all manner of critical infrastructure.

MITRE continues to be committed to CVE as a global resource. We thank you as a member of the CVE Board for your continued partnership.

Sincerely,

Yosry Barsoum
VP and Director
Center for Securing the Homeland (CSH)

CVE Program Cuts Send the Cyber Sector Into Panic Mode

After threatening to slash support for the CVE program, CISA threw MITRE a lifeline at the last minute — extending its government contract for another 11 months. After that, it looks like it's up to the private sector to find the cash to keep it going.

MITRE warns of lapse with CVE program as contract with US set to expire

The MITRE Corporation said on Tuesday that its stewardship of the CVE program — which catalogs all public cybersecurity vulnerabilities — may be ending this week because the federal government has decided not to renew its contract with the nonprofit.

U.S. Govt. Funding for MITRE's CVE Ends April 16, Cybersecurity Community on Alert

Apr 16, 2025 Ravie Lakshmanan Vulnerability Management / Incident Response

Home > News > Security > MITRE warns that funding for critical CVE program expires today

MITRE warns that funding for critical CVE program expires today

By Sergiu Gatlan April 16, 2025 02:16 AM 1

INNOVATION > CYBERSECURITY

CVE Program Funding Reinstated—What It Means And What To Do Next

By Kate O'Flaherty, Senior Contributor. Kate O'Flaherty is a cybersecurity an... Follow Author

Apr 16, 2025, 11:08am EDT

MSSP, Critical Infrastructure Security, Application security, Vulnerability Management

CISA Extends Funding for MITRE CVE Program Just as It was to Expire

April 16, 2025 Share

CISA extends funding to ensure 'no lapse in critical CVE services'

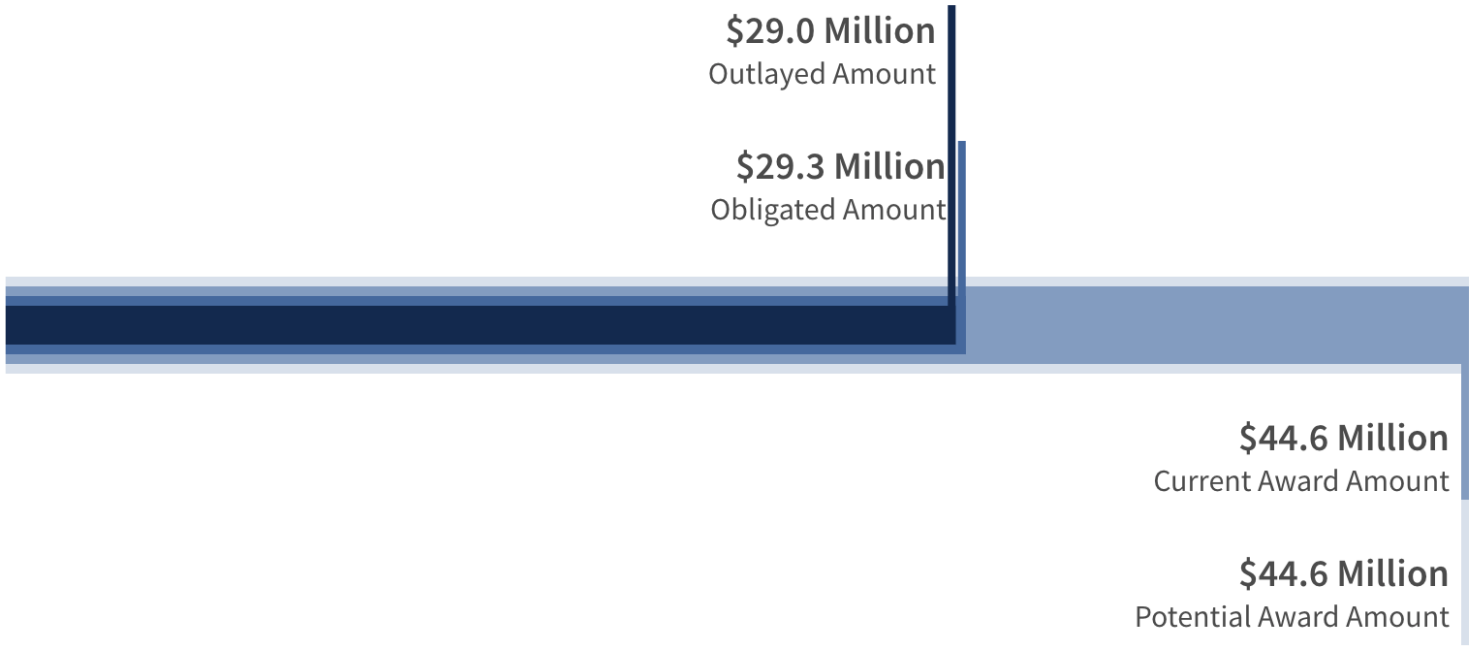
By Sergiu Gatlan April 16, 2025 09:05 AM 2

Mitre CVE program regains funding as renewal deal reached

The information security industry feared a lapse would lead to industrywide exposures of software vulnerabilities.

$ Award Amounts

Overall Spending | COVID-19 Spending



Outlayed Amount	$28,967,283.11
Obligated Amount	$29,275,363.60
Current Award Amount	$44,617,273.00
Potential Award Amount	$44,617,273.00

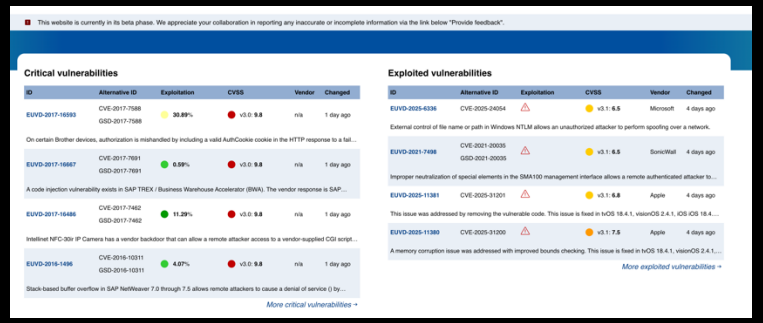
GCVE.eu

GCVE: Global CVE Allocation System

The **Global CVE (GCVE)** allocation system is a new, decentralized approach to vulnerability identification and numbering, designed to improve flexibility, scalability, and autonomy for participating entities.

While remaining compatible with the traditional CVE system, GCVE introduces **GCVE Numbering Authorities (GNAs)**. GNAs are independent entities that can allocate identifiers without relying on a centralised block distribution system or rigid policy enforcement.

Explore



FOR IMMEDIATE RELEASE

April 16, 2025

CVE Foundation Launched to Secure the Future of the CVE Program

[Bremerton, Washington] – The CVE Foundation has been formally established to ensure the long-term viability, stability, and independence of the Common Vulnerabilities and Exposures (CVE) Program, a critical pillar of the global cybersecurity infrastructure for 25 years.

Since its inception, the CVE Program has operated as a U.S. government-funded initiative, with oversight and management provided under contract. While this structure has supported the program's growth, it has also raised longstanding concerns among members of the CVE Board about the sustainability and neutrality of a globally relied-upon resource being tied to a single government sponsor.

This concern has become urgent following an April 15, 2025 letter from MITRE notifying the CVE Board that the U.S. government does not intend to renew its contract for managing the program. While we had hoped this day would not come, we have been preparing for this possibility.

In response, a coalition of longtime, active CVE Board members have spent the past year developing a strategy to transition CVE to a dedicated, non-profit foundation. The new CVE Foundation will focus solely on continuing the mission of delivering high-quality vulnerability identification and maintaining the integrity and availability of CVE data for defenders worldwide.

The CVE System

HSSEDI

Homeland Security Systems Engineering & Development Institute™

MITRE

CVE®

NIST

NVD

ANALYGENCE

CVE Program

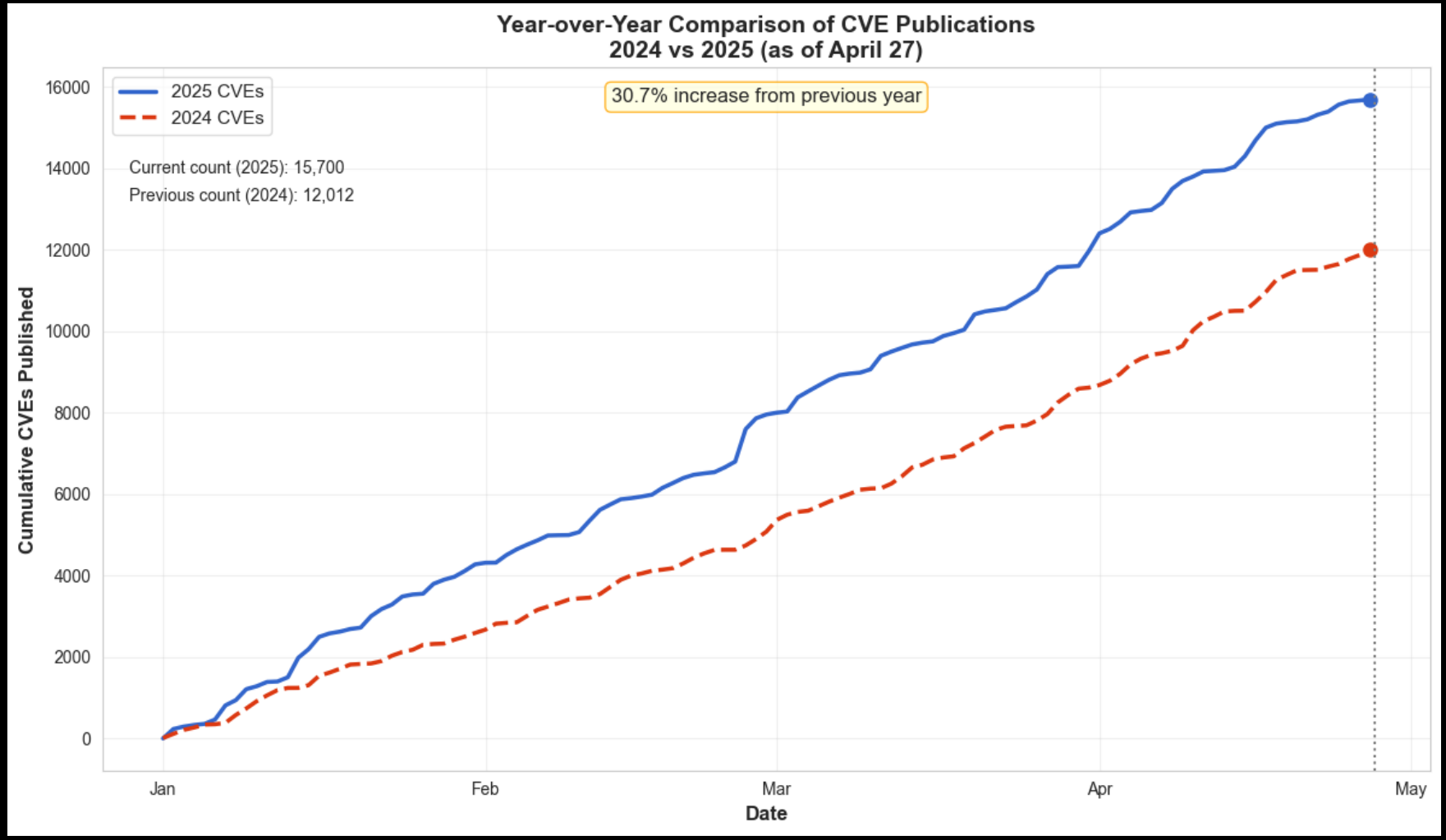
- Oversees the Public Database at CVE.org
- Upholds the CVE Publishing Rules
- Administers the CVE CNA (CVE Numbering Authorities) Program
- Operates Working Groups
  - Automation Working Group (AWG)
  - Quality Working Group (QWG)
  - Tactical Working Group (TWG)
  - CVE Artificial Intelligence Working Group (CVEAI WG)

NVD Program

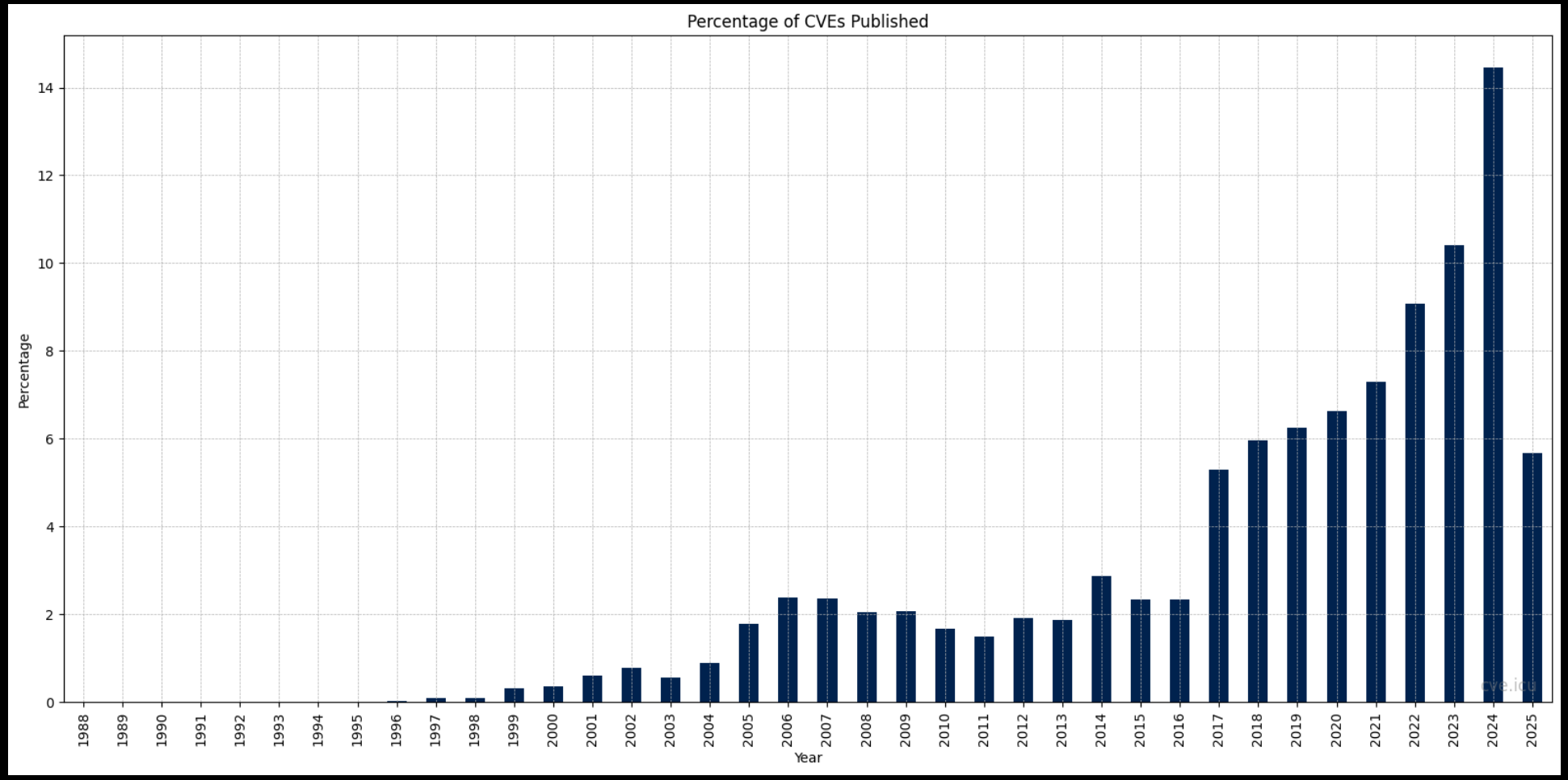
- Enhances Published CVE Records:
  - Common Weakness Enumeration (CWE)
  - Common Platform Enumeration (CPE)
  - Common Vulnerability Scoring System (CVSS)
- Primary Source of CVE Data
- Offers Official Spanish Translation Of CVEs
  - Spanish National Cybersecurity Institute (INCIBE)

Growing Crisis

Explosive CVE Growth



Explosive CVE Growth



Minimal Required Fields

cna **Required**

root > oneOf > Published > containers > cna

Type: object

An object containing the vulnerability information provided by a CVE Numbering Authority (CNA) for a published CVE ID. There can only be one CNA container per CVE record since there can only be one assigning CNA. The CNA container must include the required information defined in the CVE Rules, which includes a product, version, problem type, prose description, and a reference.

No Additional Properties

providerMetadata	**Required**
dateAssigned	
datePublic	
title	
descriptions	**Required**
affected	**Required**
problemTypes	
references	**Required**
impacts	
metrics	
configurations	
workarounds	
solutions	
exploits	
timeline	
credits	
source	
tags	
taxonomyMappings	
^x_[^.]*$	**Pattern Property**

Minimal Rules

```
"description": {
    "type": "object",
    "description": "Text in a particular language with optional alternate markup or formatted representation (e.g., Markdown) or embedded media.",
    "properties": {
        "lang": {"$ref": "#/definitions/language"},
        "value": {
            "type": "string",
            "description": "Plain text description.",
            "minLength": 1,
            "maxLength": 4096
        },
```

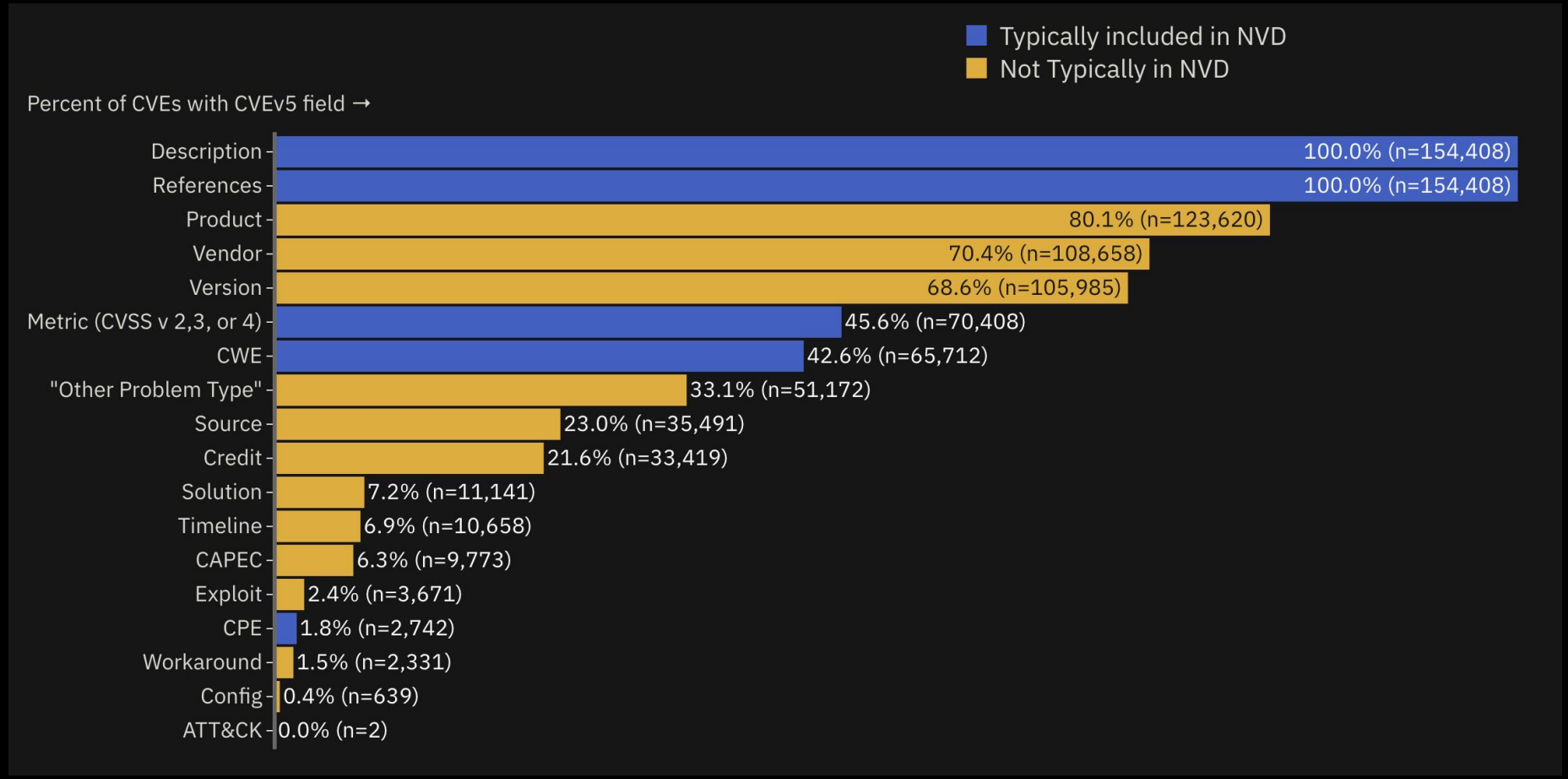
Minimal Adherence

CNA	CVE	Description
Microsoft	CVE-2025-21314	Windows SmartScreen Spoofing Vulnerability
Microsoft	CVE-2025-21308	Windows Themes Spoofing Vulnerability
Microsoft	CVE-2025-21259	Microsoft Outlook Spoofing Vulnerability
Microsoft	CVE-2025-21217	Windows NTLM Spoofing Vulnerability
Citrix	CVE-2024-6677	Privilege escalation in uberAgent
Microsoft	CVE-2024-43609	Microsoft Office Spoofing Vulnerability
Microsoft	CVE-2024-43450	Windows DNS Spoofing Vulnerability
Microsoft	CVE-2024-38200	Microsoft Office Spoofing Vulnerability
Microsoft	CVE-2024-38030	Windows Themes Spoofing Vulnerability
Microsoft	CVE-2024-38020	Microsoft Outlook Spoofing Vulnerability
Microsoft	CVE-2024-37968	Windows DNS Spoofing Vulnerability

Minimal-Minimal Adherence


```
"affected": [
    {
        "vendor": "n/a",
        "product": "n/a",
        "versions": [
            {
                "version": "n/a",
                "status": "affected"
            }
        ]
    }
],
```

Missing Product Data



https://bjedwards.observablehq.cloud/measuring-cna-performance

NVD 2024

May 29, 2024: NVD General Update

NIST has awarded a contract for additional processing support for incoming Common Vulnerabilities and Exposures (CVEs) for inclusion in the National Vulnerability Database. We are confident that this additional support will allow us to return to the processing rates we maintained prior to February 2024 within the next few months.

In addition, a backlog of unprocessed CVEs has developed since February. NIST is working with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to facilitate the addition of these unprocessed CVEs to the NVD. We anticipate that that this backlog will be cleared by the end of the fiscal year.

As we shared earlier, NIST is also working on ways to address the increasing volume of vulnerabilities through technology and process updates. Our goal is to build a program that is sustainable for the long term and to support the automation of vulnerability management, security measurement and compliance.

With a 25-year history of providing this database of vulnerabilities to users around the world and given that we do not play an enforcement or oversight role, NIST is uniquely suited to manage the NVD. NIST is fully committed to maintaining and modernizing this important national resource that is vital to building and maintaining trust in information technology and fostering innovation.

Moving forward, we will keep the community informed of our progress toward normal operational levels and our future modernization plans.

NVD 2025

- **March 19, 2025: NVD General Update**

  This update provides information on our progress as we work to process incoming CVEs and to address the backlog of CVEs that have not been fully processed:

  We are currently processing incoming CVEs at roughly the rate we had sustained prior to the processing slowdown in spring and early summer of 2024. However, CVE submissions increased 32 percent in 2024, and that prior processing rate is no longer sufficient to keep up with incoming submissions. As a result, the backlog is still growing.

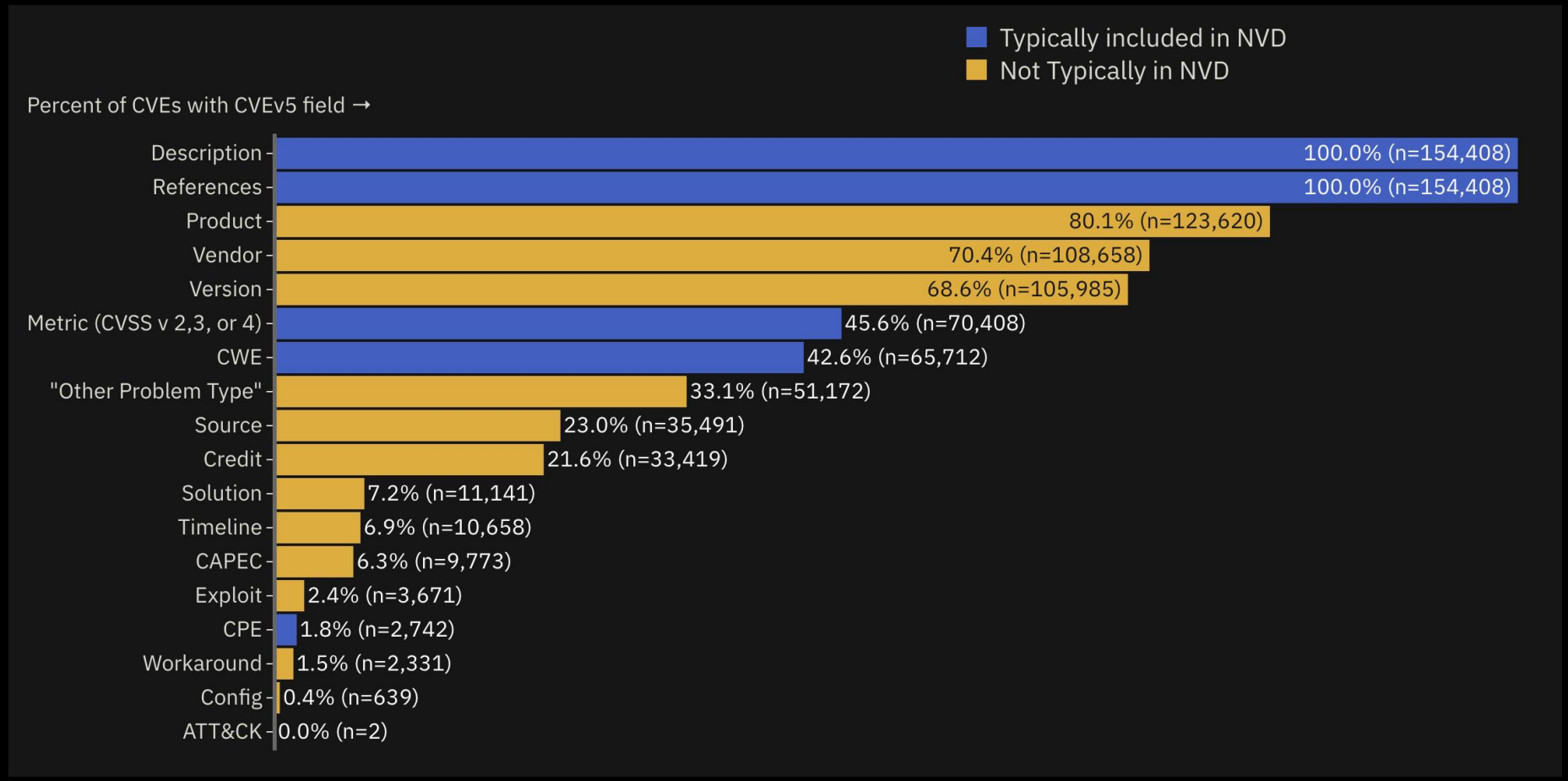
  We anticipate that the rate of submissions will continue to increase in 2025. The fact that vulnerabilities are increasing means that the NVD is more important than ever in protecting our nation's infrastructure. However, it also points to increasing challenges ahead.

  To address these challenges, we are working to increase efficiency by improving our internal processes, and we are exploring the use of machine learning to automate certain processing tasks.

CVE Status Count

Total	291518
Received	362
Awaiting Analysis	24456
Undergoing Analysis	9608
Modified	134986
Deferred	94600
Rejected	15051

Missing CVSS and CWE Data



https://bjedwards.observablehq.cloud/measuring-cna-performance

Bureaucracy, Funding & Mandates

HSSEDI

Homeland Security Systems Engineering & Development Institute™

MITRE

CVE

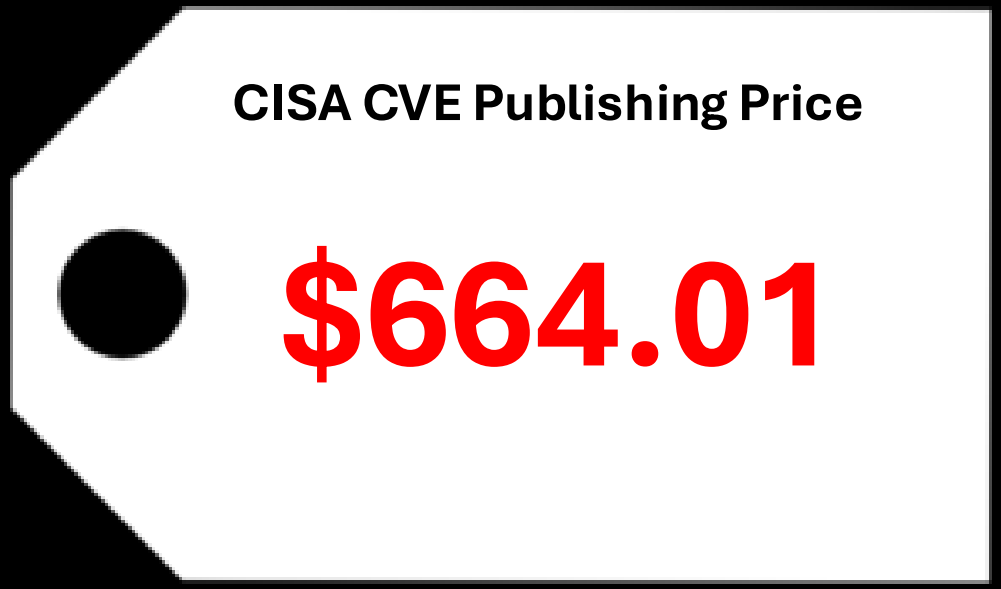
$29 Million

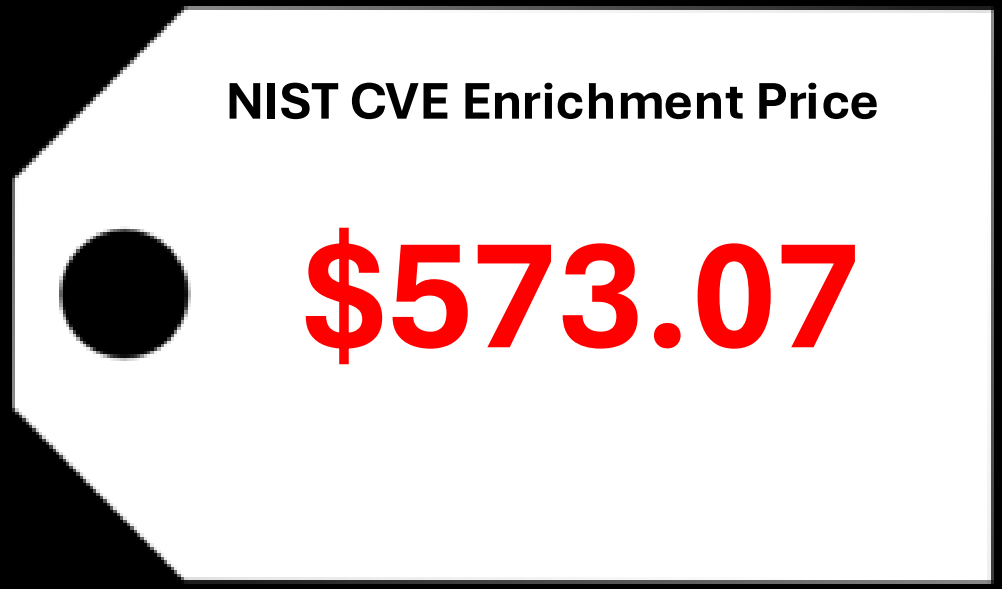
NIST

NVD

ANALYGENCE

$25 Million





For 43,625 CVEs Published From April 17, 2024, to **April 16, 2025**

Total US Government CVE Publishing Price

$1,237.07

For 43,625 CVEs Published From April 17, 2024, to **April 16, 2025**

For 290,834 CVEs in Database (End Date April 16, 2025)

Total US Government CVE Record Management Price

$188.22

For 290,834 CVEs in Database (End Date April 16, 2025)

Federally Funded Research and Development Centers

- HSOAC
- **HSSEDI**
  - Caldera and Extension for Operational Technology
  - Decider Tool for Mapping Adversary Behavior to MITRE ATT&CK® Framework
  - Drone Range for Advancing UAS Technology
  - SIMEX

Homeland Security Systems Engineering and Development Institute

The Homeland Security Act of 2002 authorized the Secretary of Homeland Security, acting through the Under Secretary for Science and Technology (USST), to establish one or more Federally Funded Research and Development Centers (FFRDCs) to provide independent analysis of homeland security issues, or to carry out other responsibilities under the Act. In 2009, the MITRE Corporation was selected to operate the Homeland Security Systems Engineering and Development Institute (HSSEDI) FFRDC. DHS established HSSEDI to serve as its primary systems engineering resource and to meet DHS-wide demand for rapid access to deep technical expertise.

Unique Purpose and Operation

HSSEDI provides specialized independent and objective technical and systems engineering expertise to DHS components, program managers and operating elements, while addressing national homeland security system

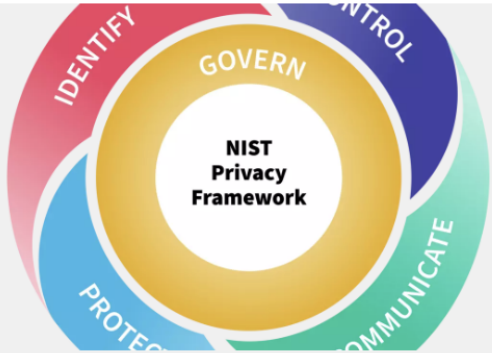
INFORMATION TECHNOLOGY LABORATORY

Cultivating Trust in IT and Metrology

About ITL
How to Work With Us
Publications
Priority Areas
Products and Services
News & Updates
Events
Standards Activities
Videos
Blogs

Full menu

2025 NICE Conference & Expo Agenda is Now Live!



NIST Updates Privacy Framework

NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption

WELCOME TO THE INFORMATION TECHNOLOGY LABORATORY

The Information Technology Laboratory (ITL) is one of NIST's six research laboratories. ITL focuses on IT measurements, testing, and standards, and is a globally recognized and trusted source of high-quality, independent, and unbiased research and data. ITL's mission, to cultivate trust in information technology (IT) and metrology, is accomplished using its world-class measurement and testing facilities and encompassing a wide range of areas of computer science,

Privatization & Globalization

GitHub Advisory Database

Security vulnerability database inclusive of CVEs and GitHub originated security advisories from the world of open source software.

GitHub reviewed advisories

All reviewed	22,372
Composer	4,669
Erlang	34
GitHub Actions	26
Go	2,261
Maven	5,512
npm	3,910
NuGet	704
pip	3,680
Pub	12
RubyGems	915
Rust	943
Swift	38

Unreviewed advisories

All unreviewed	253,333

Search by CVE/GHSA ID, package, severity, ecosystem, credit...

22,372 advisories Severity CWE Sort

Moodle allows IDOR when accessing the cohorts report Moderate
CVE-2025-3647 was published for moodle/moodle (Composer) 2 days ago

Moodle's AJAX section delete does not respect course_can_delete_section() Moderate
CVE-2025-3644 was published for moodle/moodle (Composer) 2 days ago

Moodle's mod_data edit/delete pages pass CSRF token in GET parameter Low
CVE-2025-3637 was published for moodle/moodle (Composer) 2 days ago

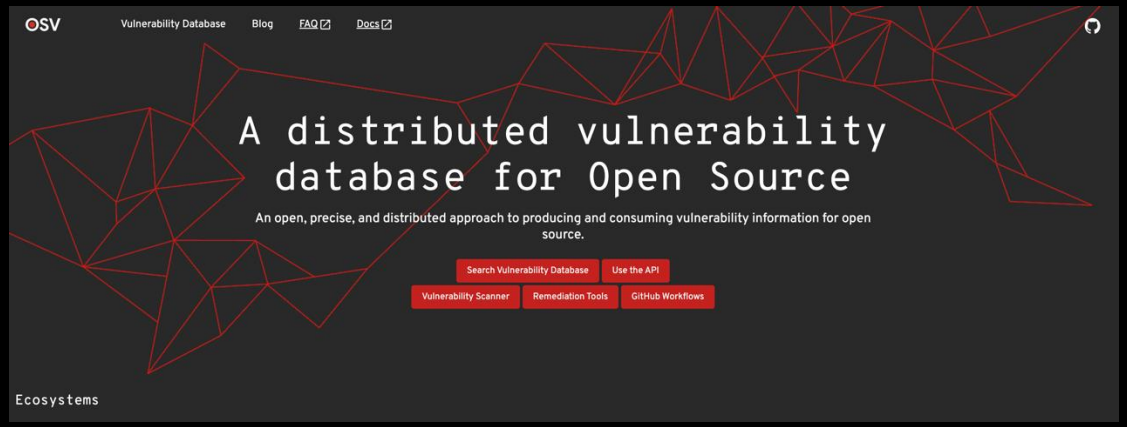
Moodle has an IDOR in messaging web service which allows access to some user details Moderate
CVE-2025-3645 was published for moodle/moodle (Composer) 2 days ago

Moodle has an authenticated remote code execution risk in the Moodle LMS EQUELLA repository High
CVE-2025-3642 was published for moodle/moodle (Composer) 2 days ago

Moodle has an IDOR in web service which allows users enrolled in a course to access some details of other users Moderate
CVE-2025-3640 was published for moodle/moodle (Composer) 2 days ago

Moodle has a CSRF risk in Brickfield tool's analysis request action Low
CVE-2025-3638 was published for moodle/moodle (Composer) 2 days ago

Moodle has reflected Cross-site Scripting risk in policy tool Moderate
CVE-2025-3643 was published for moodle/moodle (Composer) 2 days ago



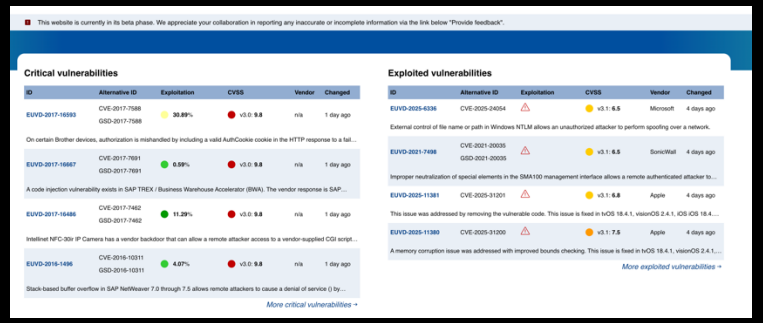
GCVE.eu

GCVE: Global CVE Allocation System

The **Global CVE (GCVE)** allocation system is a new, decentralized approach to vulnerability identification and numbering, designed to improve flexibility, scalability, and autonomy for participating entities.

While remaining compatible with the traditional CVE system, GCVE introduces **GCVE Numbering Authorities (GNAs)**. GNAs are independent entities that can allocate identifiers without relying on a centralised block distribution system or rigid policy enforcement.

Explore



FOR IMMEDIATE RELEASE

April 16, 2025

CVE Foundation Launched to Secure the Future of the CVE Program

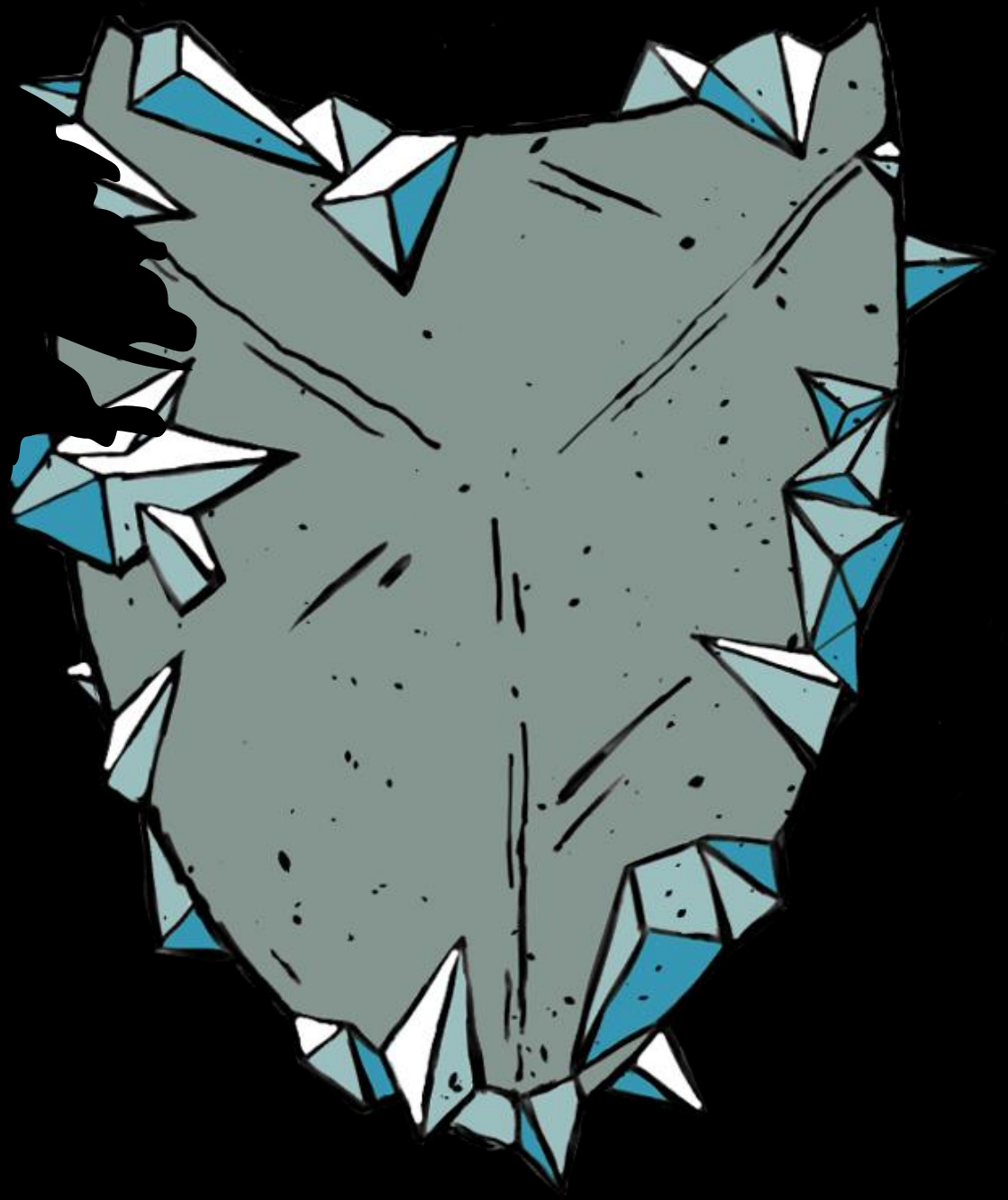
[Bremerton, Washington] – The CVE Foundation has been formally established to ensure the long-term viability, stability, and independence of the Common Vulnerabilities and Exposures (CVE) Program, a critical pillar of the global cybersecurity infrastructure for 25 years.

Since its inception, the CVE Program has operated as a U.S. government-funded initiative, with oversight and management provided under contract. While this structure has supported the program's growth, it has also raised longstanding concerns among members of the CVE Board about the sustainability and neutrality of a globally relied-upon resource being tied to a single government sponsor.

This concern has become urgent following an April 15, 2025 letter from MITRE notifying the CVE Board that the U.S. government does not intend to renew its contract for managing the program. While we had hoped this day would not come, we have been preparing for this possibility.

In response, a coalition of longtime, active CVE Board members have spent the past year developing a strategy to transition CVE to a dedicated, non-profit foundation. The new CVE Foundation will focus solely on continuing the mission of delivering high-quality vulnerability identification and maintaining the integrity and availability of CVE data for defenders worldwide.

Proposed Solutions



Quality Validation Processes

All CVEs should pass a well documented and maintained quality validation test before automated publication.

Enhanced Publication Requirements

- More Mandatory Fields For CVE Publishing
  - CVSS
  - CPE
  - CWE
- Plain or Markdown Advisories
  - Future Proof CVEs

Government Efficiency

Merge the initiatives of CISA and NIST into one entity that will disseminate, enhance, and supply vulnerability information to the public.

Call To Action

Call To Action

- Advocate for Improved Data Quality from CNAs
- Participate in a Working Group
- Lobby Government Representatives
  - Ensure Funding
  - Combine The NVD and MITRE

Thank You!

Jerry Gamblin

jerry.gamblin@gmail.com

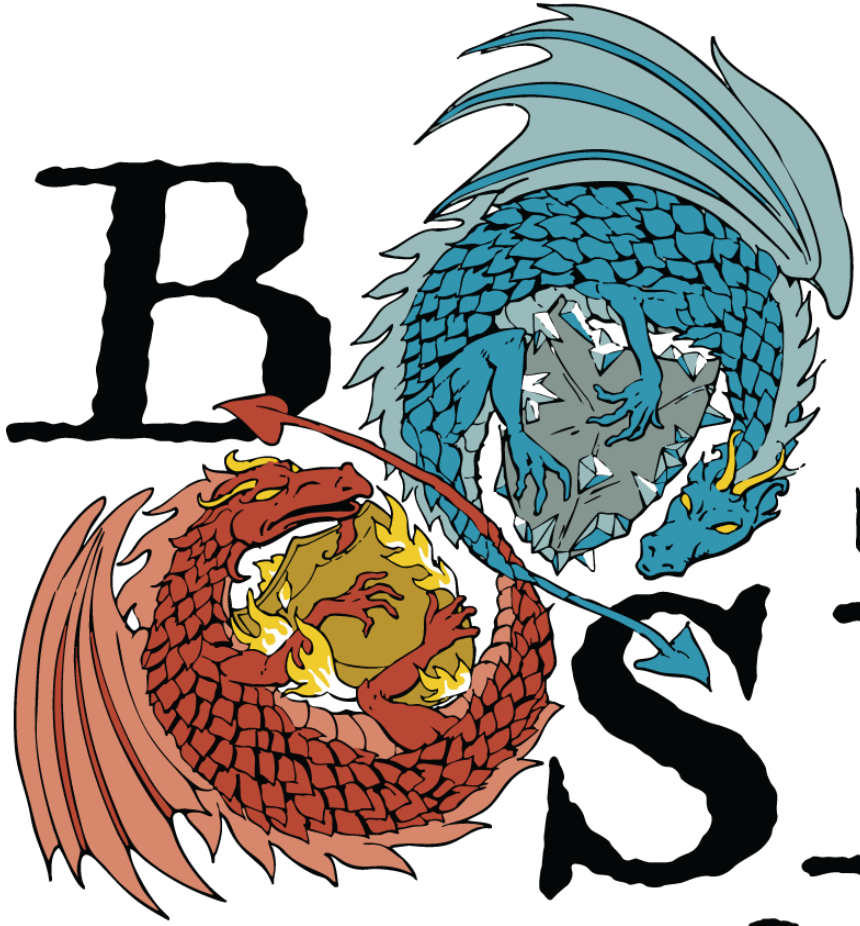
@jgamblin (X/Etc)

jerrygamblin.com

cve.icu

Q&A
(via Slido)

Feedback
(2 questions)



BSIDES San Francisco 2025