

# Demystifying the CVE Program: Understanding Its Role and Uncertain Future

Mohannad Alhanahnah

[Mohannad.Alhanahnah@chalmers.se](mailto:Mohannad.Alhanahnah@chalmers.se)

# What is a CVE?



CVE = Common Vulnerabilities and Exposures



Public list of known cybersecurity issue



Components of a CVE Record

CVE-ID

Assigning CNA

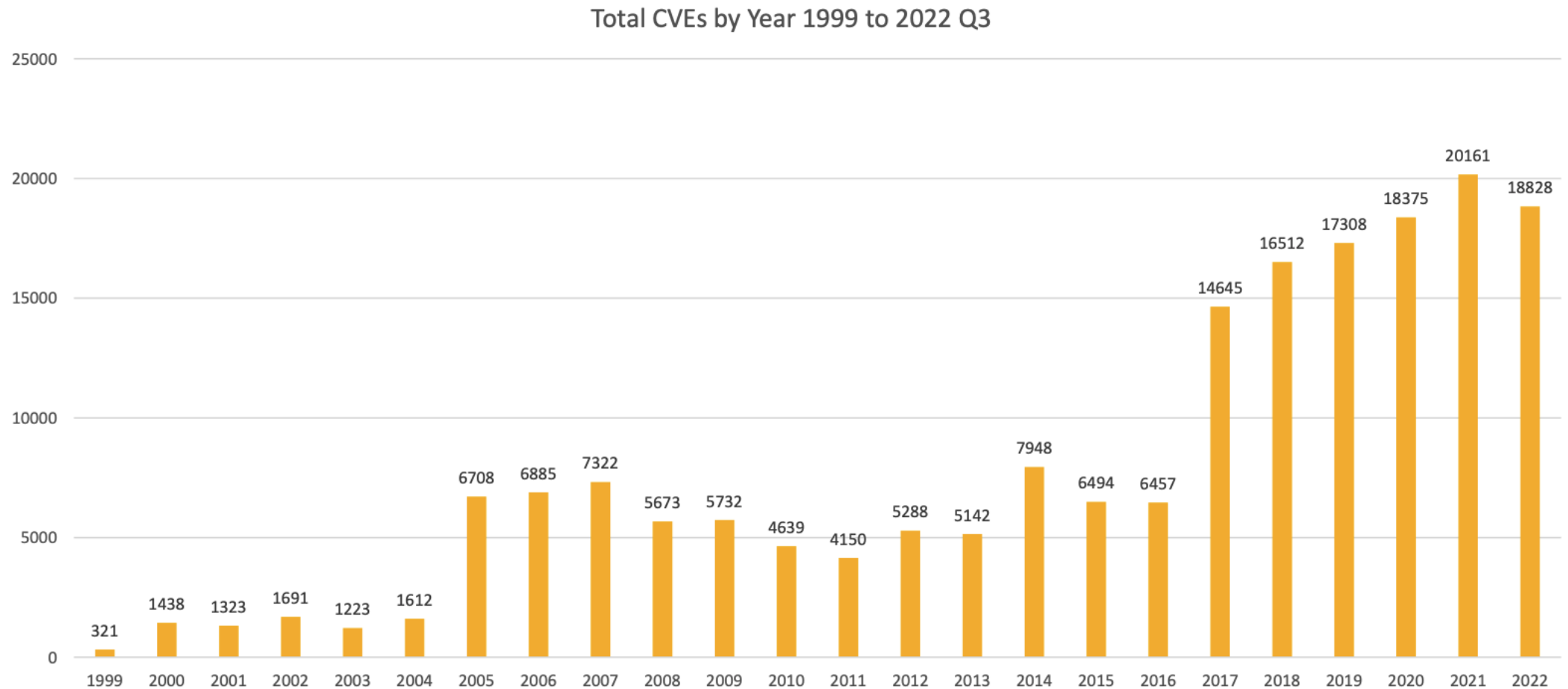
Description

Record created date

References

CVE-ID	
<b>CVE-2017-15125</b>	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
A flaw was found in CloudForms before 5.9.0.22 in the self-service UI snapshot feature where the name field is not properly sanitized for HTML and JavaScript input. An attacker could use this flaw to execute a stored XSS attack on an application administrator using CloudForms. Please note that CSP (Content Security Policy) prevents exploitation of this XSS however not all browsers support CSP.	
References	
<b>Note:</b> <a href="#">References</a> are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"><li>BID:102287</li><li>URL:<a href="http://www.securityfocus.com/bid/102287">http://www.securityfocus.com/bid/102287</a></li><li>CONFIRM:<a href="https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-15125">https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-15125</a></li><li>REDHAT:RHSA-2018:0380</li><li>URL:<a href="https://access.redhat.com/errata/RHSA-2018:0380">https://access.redhat.com/errata/RHSA-2018:0380</a></li></ul>	
Assigning CNA	
Red Hat, Inc.	
Date Record Created	
<b>20171008</b>	Disclaimer: The <a href="#">record creation date</a> may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

# CVE Numbers Growth



# CVE Program



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



The program was started in 1999, funded by the U.S. Federal Government



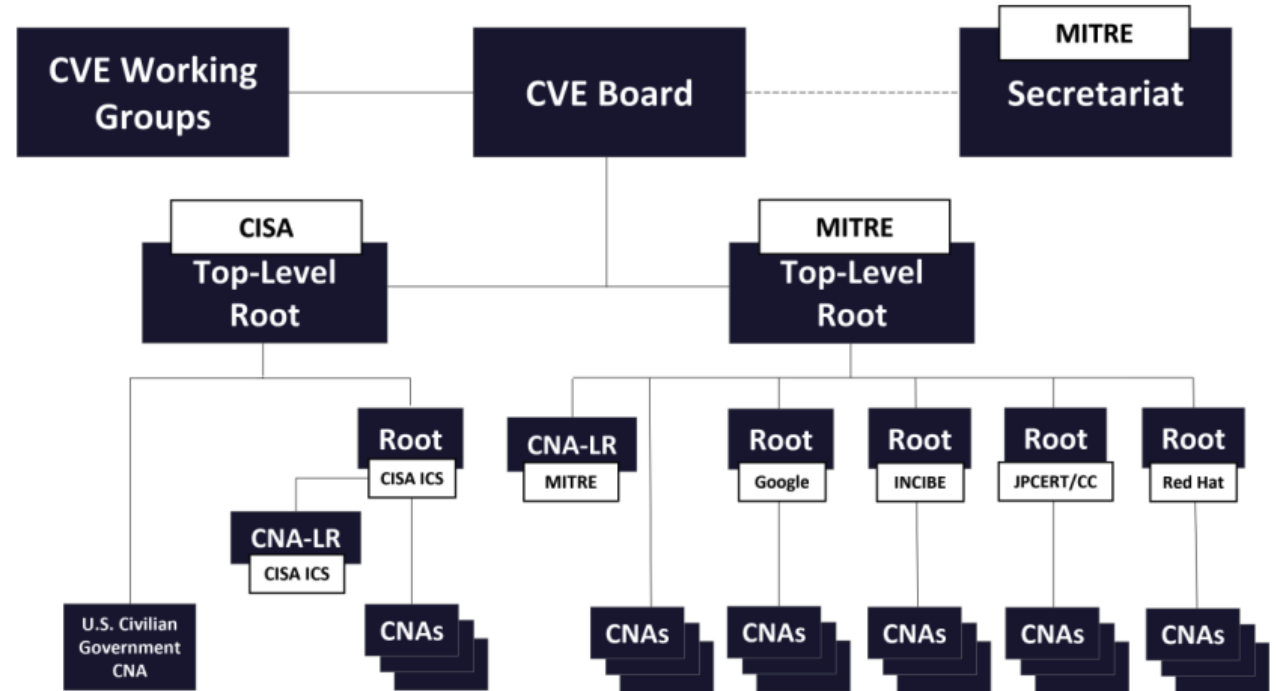
The MITRE Corporation is paid by the U.S. Federal Government to administer the CVE Program



The CVE Program is a global community effort managed by the CVE Board

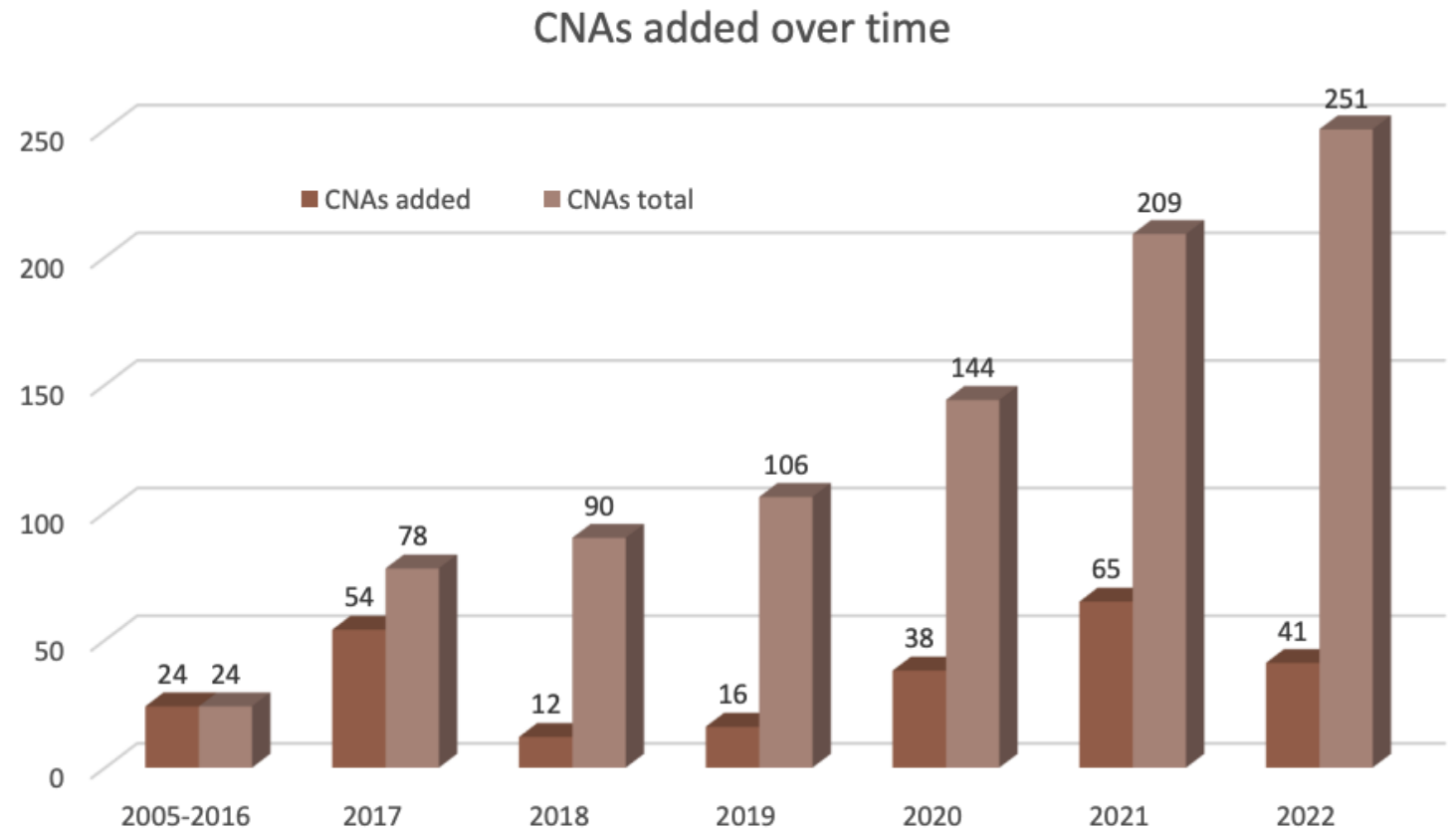
# CVE Program Organization

- **CVE Board:** The organization responsible for the strategic direction, governance, operational structure, policies, and rules of the CVE Program.
- **CNA:** An organization responsible for the regular assignment of CVE IDs to vulnerabilities, and for creating and publishing information about the vulnerability in the associated CVE Record. Each CNA has a specific Scope of responsibility for vulnerability identification and publishing.
- **Root:** 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 Root:** A Root that does not report to another Root, and is thus responsible to the CVE Board.
- **CVE Working Group:** An organization created and administered by the CVE Board to accomplish specific objectives through collaboration with CVE stakeholders and the general public where appropriate. Each working group is required to have a charter which defines its area of responsibility, membership, and objectives



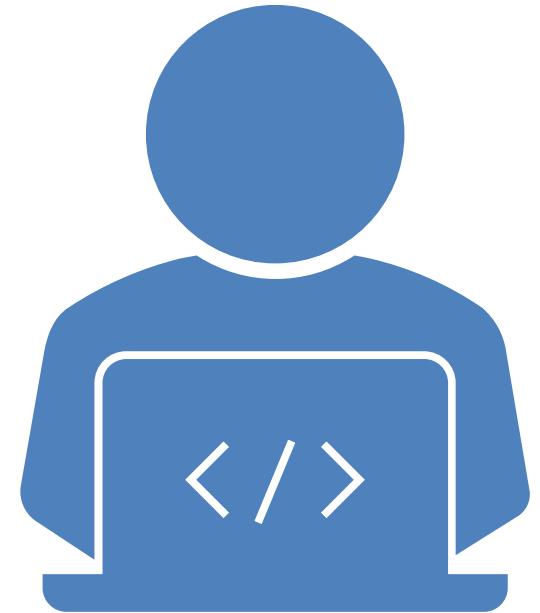
# Participants Growth

- 251 total partners
- 35 countries

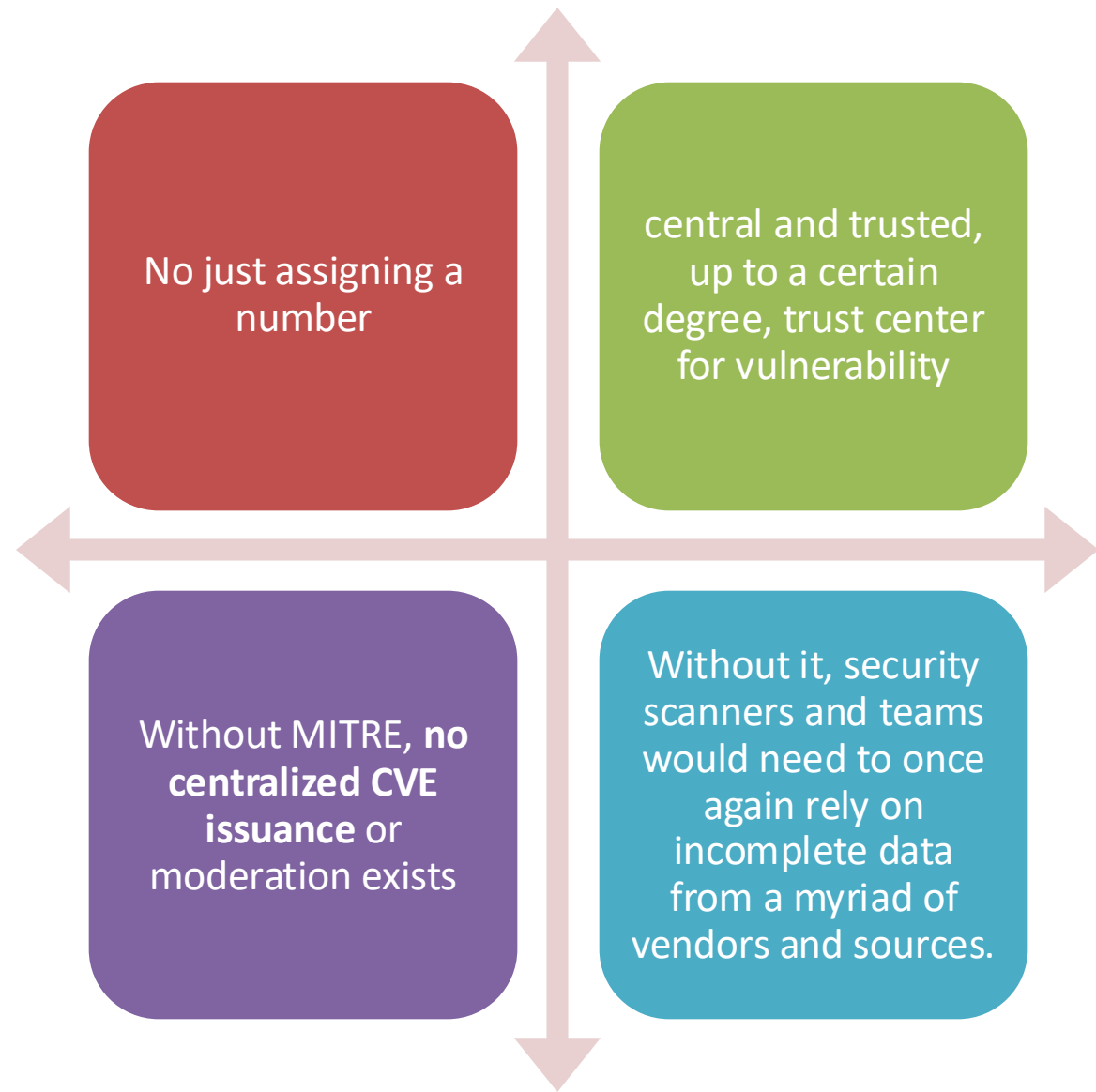


# Who Operates CVE?

- The MITRE Corporation operates the CVE program, which is funded by the US Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Vulnerability Management Component (VMC).



# Importance of CVEs



# Promoted other projects

- The official CVE list does not include an assessment of the severity of each CVE. Other organizations that maintain their own lists of CVEs, most notably [NIST's National Vulnerability Database \(NVD\)](#), assign severity categories (such as “medium,” “high” and “critical”) and/or numerical severity scores to CVEs.

# I'm just a Vuln: How a disclosure becomes a finding

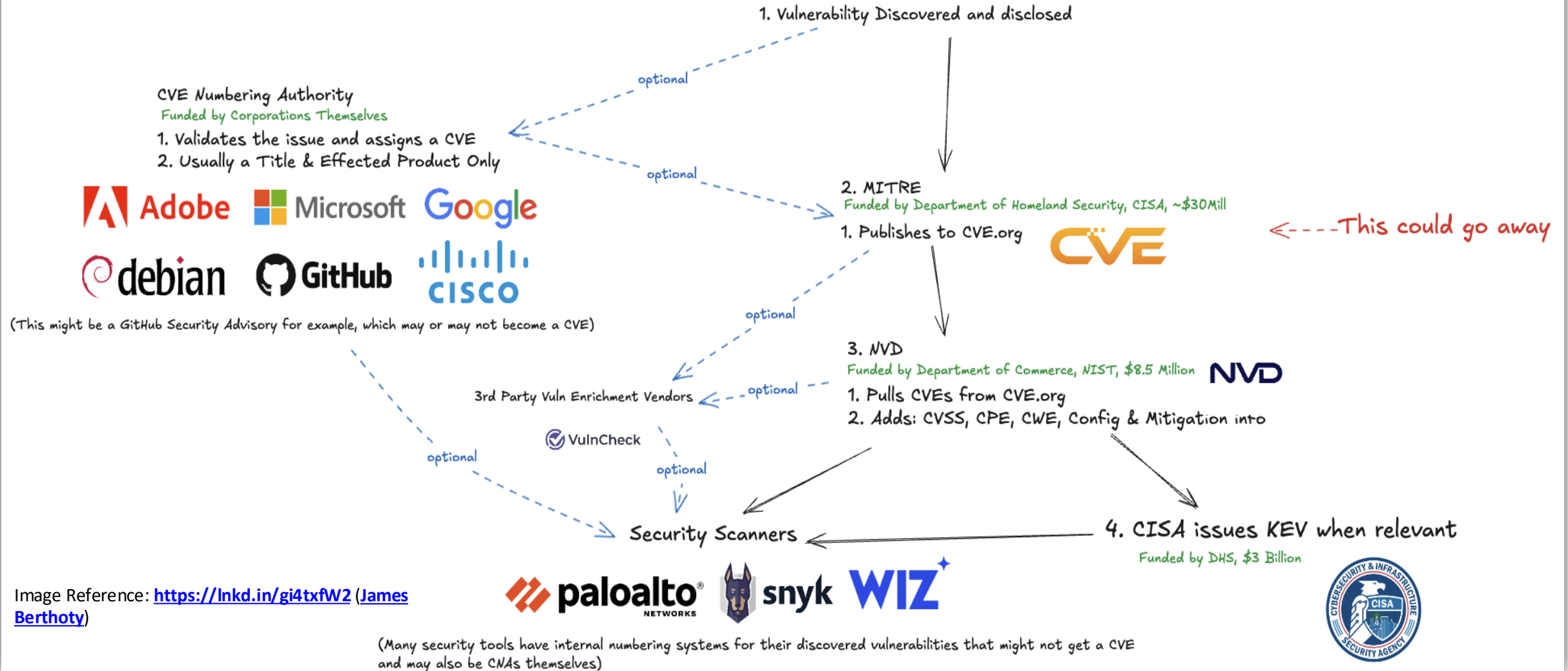
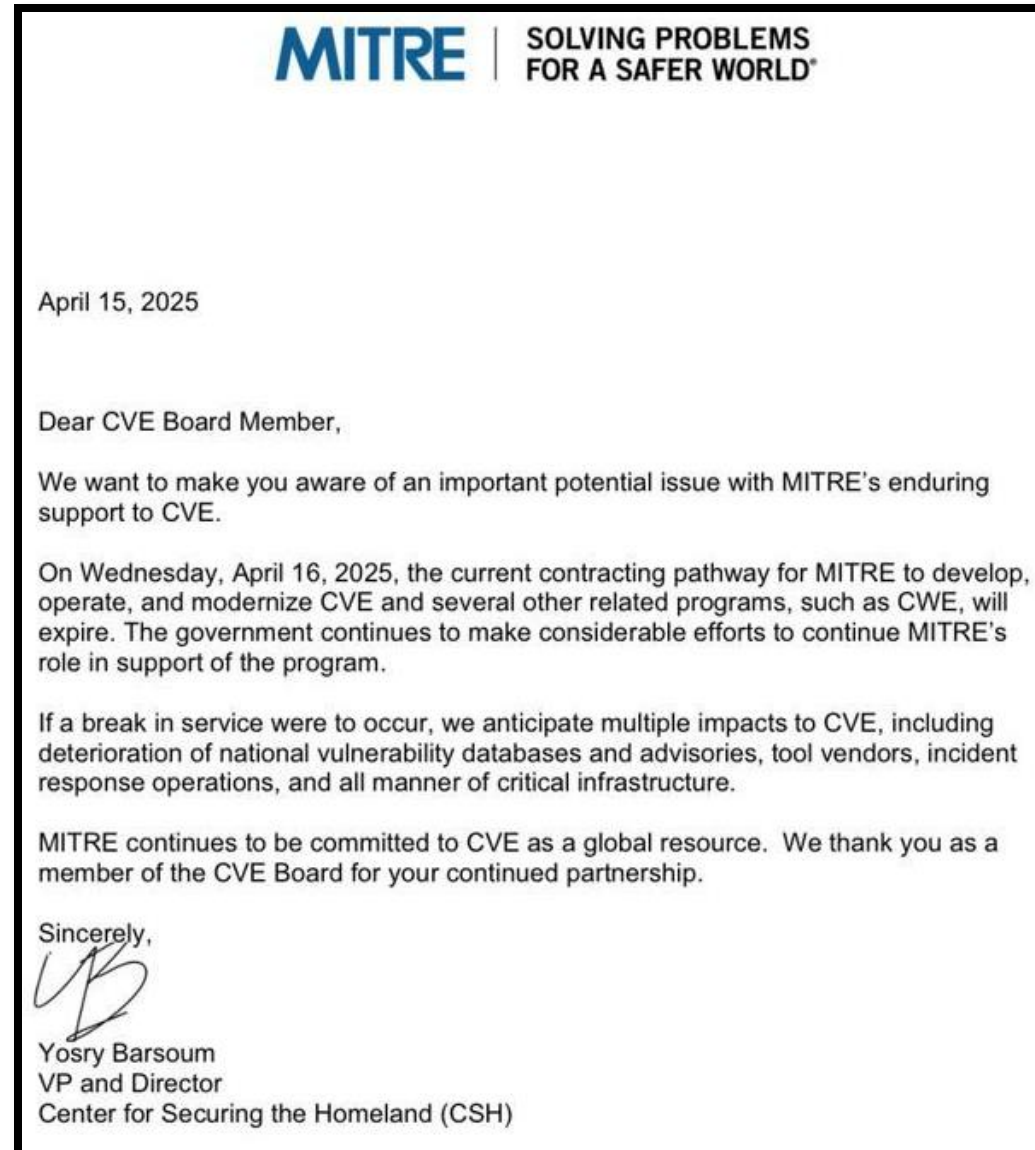


Image Reference: <https://lnkd.in/gi4txfW2> (James Berthoty)

# MITRE's support of the CVE program is at risk



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.

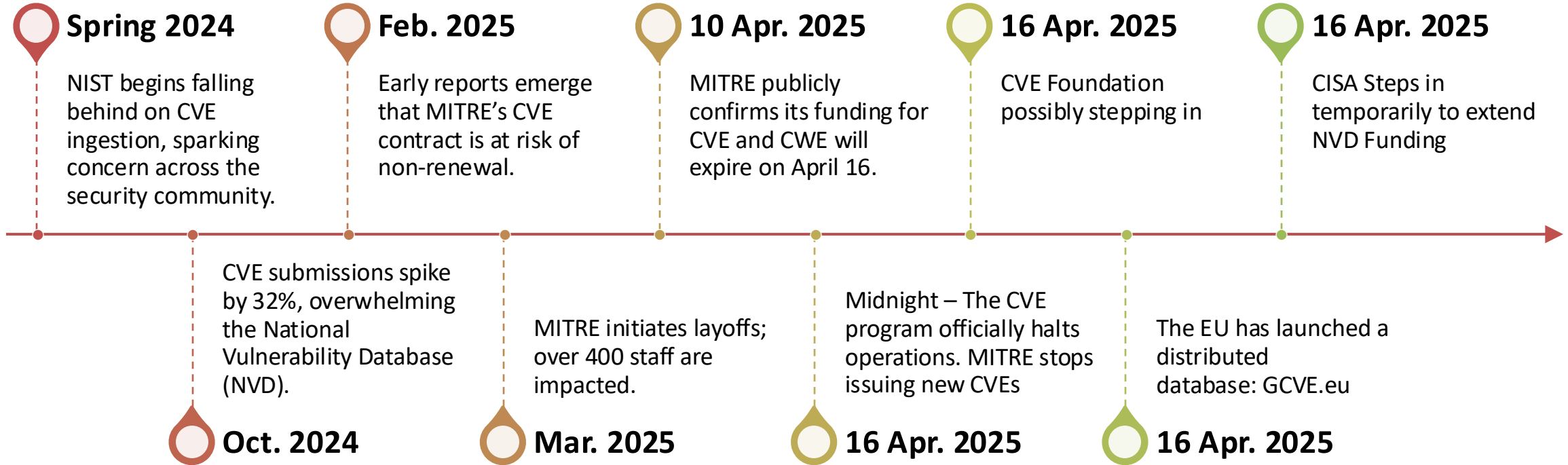
MITRE continues to be committed to CVE as a global resource. We thank you as a member of the CVE Board for your continued partnership.

Sincerely,

A handwritten signature in black ink, appearing to be "YB", is written over the printed name.

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

# Timeline of Events



# What is the Impact?

Former CVE board member **Brian Martin** outlined a multi-level impact:

- **CNAs (CVE Numbering Authorities)** can no longer efficiently assign IDs.
- The already-overwhelmed **NVD** (with 30,000+ backlogged vulnerabilities) loses its authoritative source of new CVEs.
- Commercial databases that rely on MITRE's CVE program will face severe intelligence gaps.
- International vulnerability exchanges, including in **Russia** and **China**, will be cut off from consistent CVE data.
- Thousands of **CERTs** and security teams globally will lose a free, reliable source of vulnerability intelligence.

# Some Reactions

the CVE database and API for new CVEs from CNAs will continue working, but other slowdowns will happen when it comes to getting CVEs from MITRE themselves for non-CNAs.

Without new CVEs flowing in, **NVD loses relevance rapidly**

historical CVE records will be available at GitHub, <https://lnkd.in/e9 TE9hi>

MITRE's CVE database is likely going offline tomorrow.

I am glad to see the CVE system getting blown up

Related programs, such as the Common Weakness Enumeration (CWE™) Program, will expire

Delayed vulnerability declaration and confusion with more vulnerability scanners having their own database

**The absence of centralized, authoritative records slows threat modeling, disrupts software bill-of-materials (SBOM) tracking, and breaks automation pipelines across DevSecOps tooling.**



r/cybersecurity · 21 days ago  
edoardottt

## What is happening at MITRE?

### New Vulnerability Disclosure

I've submitted 3 new 0day vulnerabilities using the form at [cveform.mitre.org](https://cveform.mitre.org).  
More than 2 months passed and I didn't received any feedback/email/message, nothing.

For context, I've already used this process for more than 10 CVEs, does someone know why now it takes so much time to receive a response?

# Alternatives

- [CVE DB](#) on GitHub
- [OSV](#) – Google’s open-source vulnerability database
- [GitHub Security Advisories](#) – An increasingly vital source of developer-facing disclosures
- Recently emerged:
  - GCVE: Global CVE Allocation System (**GCVE.eu**)
    - decentralized approach to vulnerability identification and numbering
  - EU vulnerability database [EUVD](#)
  - Vulnerability-Lookup <https://vulnerability.circl.lu/>
- [CVE Tracker](#)

# Emerging Initiatives and discussions

- CVE records will continue to be available at [github](#). Brian Krebs [says](#) the API that CNAs use to get CVEs will remain available.
- Josh Bressers has set up a discord, [Extended Vulnerability Community](#).
- Jen Easterly has a good [post](#) on Linkedin about the problems CVE solves and what'll happen without it.
- [VulnCheck commits to providing CVEs for researchers](#). Anthony Bettini was there at the start, and is a stalwart.
- [Decentralized replacement](#) to the CVE system using linked data, which can integrate with other linked data tech like SPDX 3 and OpenVEX.
- CVE Foundation (<https://www.thecvefoundation.org/>)

# CVE Program Continues Under Temporary Extension

CISA steps in at the last minute — 11-month extension granted

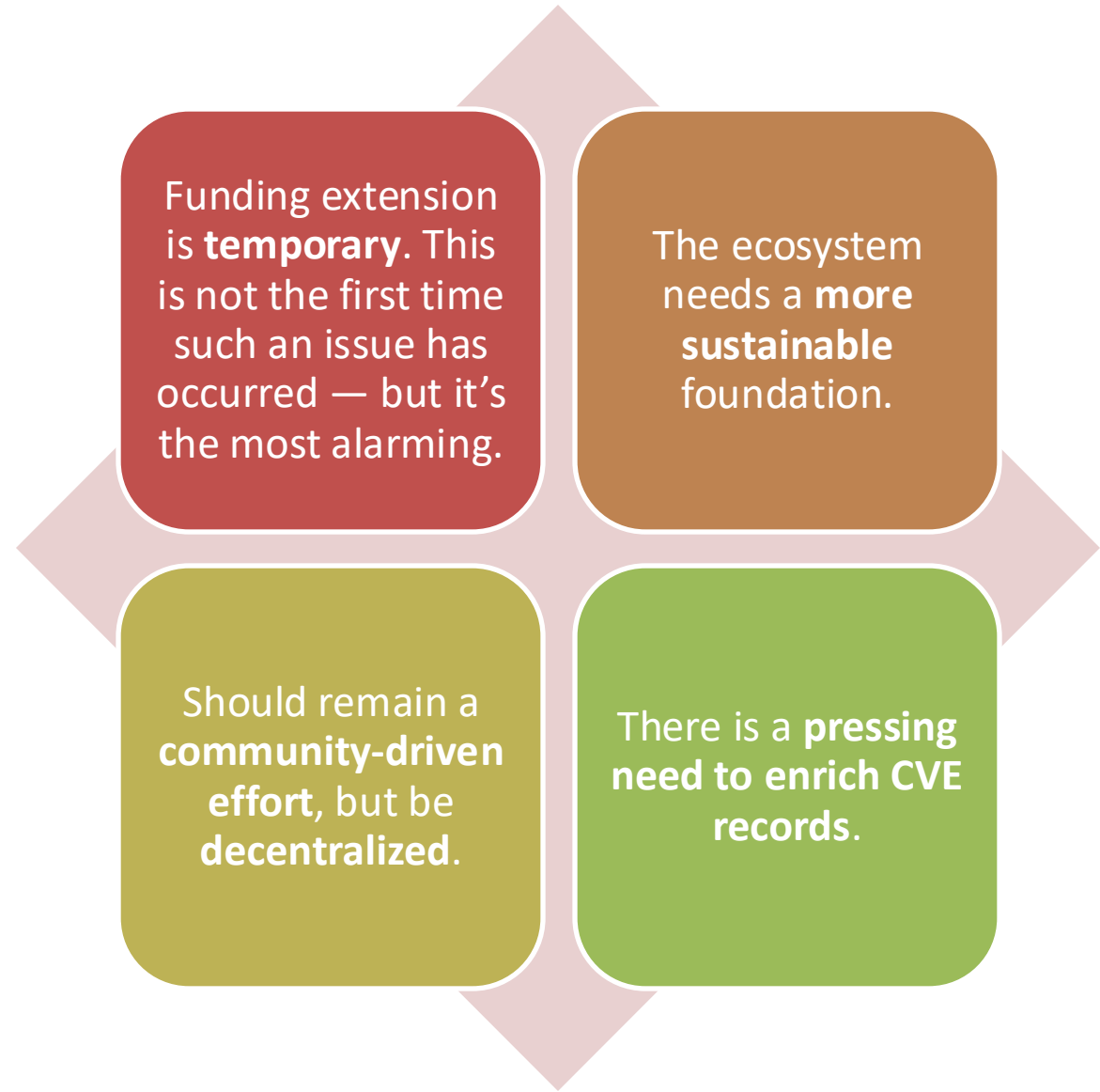
“

The CVE Program is invaluable to the cyber community and a priority of CISA. Last night, CISA executed the option period on the contract to ensure there will be no lapse in critical CVE services. We appreciate our partners' and stakeholders' patience.

”



# What This Tells Us?



# Any Suggestions?



Mohannad.Alhanahnah@chalmers.se



<https://mohannadcse.netlify.app/>



@MAIhanahnah



Mohannadcse

# References

- <https://phoenix.security/the-cve-nvd-crisis-a-wake-up-call-for-application-security/>
- [https://www.linkedin.com/posts/navid-f-rabbi\\_cybersecurity-cve-vulnerabilitymanagement-activity-7318168428995899395-OeCj/](https://www.linkedin.com/posts/navid-f-rabbi_cybersecurity-cve-vulnerabilitymanagement-activity-7318168428995899395-OeCj/)
- <https://www.linkedin.com/feed/update/urn:li:activity:7318033864096972802/>
- [https://www.linkedin.com/posts/endorlabs\\_vulnmanagement-mitre-nist-activity-7318049492820271104-G5kT](https://www.linkedin.com/posts/endorlabs_vulnmanagement-mitre-nist-activity-7318049492820271104-G5kT)
- <https://tomalrichblog.blogspot.com/2025/04/cve-circles-toilet.html?m=1>
- [https://www.reddit.com/r/cybersecurity/comments/1jk79q8/what is happening at mitre/](https://www.reddit.com/r/cybersecurity/comments/1jk79q8/what_is_happening_at_mitre/)
- <https://shostack.org/blog/thoughts-on-cve/>
- <https://thehackernews.com/2025/04/us-govt-funding-for-mitres-cve-ends.html?m=1#update-cisa-extends-cve-program-contract-amid-funding-crisis>
- [https://www.linkedin.com/posts/jdwuscg\\_maybe-an-unpopular-personal-opinion-but-activity-7318253193652547584-jZnn/](https://www.linkedin.com/posts/jdwuscg_maybe-an-unpopular-personal-opinion-but-activity-7318253193652547584-jZnn/)