

**CWE Board  
Meeting Minutes  
July 23, 2025**

## Meeting Attendance

Attendees:

- ☒ Steve M Christey (Guest)
- ☒ Bill Curtis
- ☒ Chris Eng
- ☒ Jason Fung
- ☐ Robin Gandhi
- ☒ Ganand Ganesh Kini (Guest)
- ☒ Jay Gazlay
- ☒ Alex Hoole
- ☒ Joe Jarzombek
- ☐ Jason Lam
- ☒ Jason Oberg
- ☐ Deana O'Meara
- ☐ Kurt Seifried
- ☒ Alec J. Summers
- ☐ Chris Turner
- ☐ Jeremy West

## Agenda

- Introduction
- Most Important Hardware Weaknesses
- AI CVE-CWE Benchmarking
- Top 25 Status Update
- Open Discussion

## Action Items

- None

## Topics

### Introduction

- A member kicked off the meeting by explaining the rescheduling due to the holiday and summer vacations and outlined the agenda focusing on discussion and status

updates on major ongoing efforts. The member noted that the next meeting would be a working group update.

## Most Important Hardware Weaknesses

- A member provided an update on the methodology and progress of the most important hardware weaknesses list, including data collection and expert opinions. The initiative has relied on forming a hardware weaknesses working group and collecting data from CVE and vulnerability data, security advisories, and conferences. Team members also collected expert opinions through a two-part poll. The polls aimed to gather insights from SIG members on important weaknesses.
- A member detailed the data collection process, which involved looking at CVE and vulnerability data, security advisories, and conferences. The goal was to gather comprehensive data to inform the approach to identifying the most important hardware weaknesses. The working group will meet to finalize the hardware weaknesses list, aiming to complete the list and publish it by the end of next month.
- Members also discussed the sources of known vulnerabilities influencing the ranking of the most important weaknesses, noting that there is little real data on hardware CWEs in the NVD.
- A member encouraged the board to help amplify the messaging once the list is published, noting the importance of leveraging communication channels to draw attention to it.
- Another member invited the rest of the group to share hardware exploits to understand their attack paths.

## AI CVE-CWE Benchmarking

- A member provided an update on the benchmarking effort, spotlighting assistance from a contributor who supported the work. A member noted that the effort includes participants from CNAs, AI researchers, and CWE SMEs who are working to improve root cause mapping and enhance the accuracy of an AI model in identifying CWE mappings correctly. The group aims to create a centralized chatbot within the CWE program and develop tutorial guides for setting up similar systems in different operations. Within that effort, a subgroup formed to develop the benchmarking project includes representatives from various cohorts in the CWE community.
- A member discussed the challenges of assessing the correctness of mappings in the benchmarking effort, underscoring the importance of providing partial credit for mappings that are close, but not perfect, and the need to account for hierarchical relationships between CWEs. The member also emphasized the importance of

scoring benchmarks for AI systems, explaining that the scoring should consider factors such as path distance between suggested and correct CWEs, and the level of abstraction in the mappings.

- A member also raised the issue of how AI systems should behave when presented with data that lacks weakness information. The member mentioned the need for systems to recognize when there is insufficient information to suggest a CWE, rather than making low-confidence suggestions.
- The group also discussed the value of the benchmark program to the broader CVE and CWE communities.

## Top 25 Status Update

- A member provided an update on the Top 25 project, mentioning that data was collected from NVD and vulnerability sources and includes CVEs published in the past year.
- To collect the data, the team supporting the project aims to contact CNAs and provide them with batches of CVEs to review. The CNAs will be asked to update the CWE mappings based on keyword suggestions and high-level problematic classes.
- Last year, the response rate from CNAs was around 50%, which the group aims to improve this year by giving CNAs more time to respond and providing additional AI-generated suggestions for CWE mappings. The batches will also include AI-generated suggestions for CWE mappings, which are intended to assist CNAs in making more accurate mappings.
- The project team aims to publish the Top 25 by November or early December of this year, which will depend on the response rate and the quality of the updates provided by the CNAs.
- In response to a question on the issue of CNAs intentionally submitting abstract CVE descriptions and classifications, the group discussed the potential reasons for those submissions and considered the need for a multi-stakeholder approach to ensure submissions would be relevant and balanced.
  - A member questioned whether CNAs might be doing this to balance the need for timely disclosure with the risk of providing too much detail to attackers. The member also suggested that a multi-stakeholder approach is needed to address the issue of abstract CVE submissions, emphasizing the importance of understanding the root causes and finding a balance between providing sufficient detail for defenders and minimizing risk to attackers.
- A member suggested that under certain circumstances, CNAs could release partial information in CVE records and then update the records later with full details after.

The group discussed the need to understand the root causes of issues and identify ways to reduce risks over time. The group also discussed the potential impact of the European Union Vulnerability Database on the CVE and CWE communities, leading to a discussion on the engagement with ENISA, the European Union Agency for Cybersecurity, and the alignment of databases.

- A member suggested having a more detailed discussion on the impact of the EU Vulnerability Database and the Cyber Resilience Act in future meetings, potentially involving additional stakeholders.

#### Open Discussion

- No discussion was held.

#### Next CWE Board Meeting

- August 27<sup>th</sup>, 2025