**CWE Board**
**Meeting Minutes**
**March 12, 2025**

## Meeting Attendance

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

## Agenda

- Introduction
- Upcoming CWE minor release update – April 3
  - Usability: macro- and micro- improvements
  - Content Development Repository (CDR) public release
  - CWE Chatbot, grounded LLM tool
- Open Discussion

## Action Items

- Hold a working session to explore the possibility of providing impact and likelihood values as part of the broader micro-usability updates discussion. Collaborate to gather real data to support the inclusion of likelihood information in CWE entries.
- Explore the possibility of creating machine-readable images using UML diagrams or alternatives to enhance analysis of weaknesses.
- Investigate the feasibility of creating automated links to the National Vulnerability Database (NVD) for each CWE to show all instances of a specific CWE.

- Members interested in the meeting to review weaknesses recently added to the OMG standard, hosted on Thursday, March 20th at the Hyatt Regency in Reston, VA, were encouraged to attend.

# Topics

## Introduction

- CWE Board meetings will take place every other month for an hour and a half.

## Upcoming CWE minor release update – April 3

- Micro usability updates for the release of 4.17 aim to simplify and streamline the collection and recording of individual CWE entries to minimize the amount of text that focuses on weaknesses. These changes also would move extraneous text over to other elements within CWE. This process is intended to improve the structure of records, apply a more straightforward presentation for creating images of weaknesses, preserve data, and describe the consequences.
- The team behind this effort is working on the Top 100 most requested entries. It was estimated that the number of CWE updates for the micro-usability initiative should reach 10-15 as the group works to handle the initial bottleneck of developing a solid image idea.
    - A member suggested creating machine readable images such as UML, sequence, and activity diagrams that are translatable to a model. The usability for a less technical audience makes it user-friendly. AI can be good at summarization but not necessarily classification. More formal diagrams may help users conduct analysis on similar attack patterns and underlying weaknesses.
        - There have been several attempts to conduct formal modeling, but that approach comes with its own challenges. Concerns were expressed about using AI, which in the past generated highly inaccurate results.
        - It was clarified that diagrams made independent of AI could help conduct analysis that could help verify the hierarchical structure of the CWE taxonomy and also potentially identify overlaps, perhaps between hardware CWS and legacy weakness types that could be used for merging in the future.
        - Members acknowledged the idea and considered it for future additions, noting that it would be a change in approach but could be explored further. Additional discussion considered the potential value and drawbacks of introducing vulnerability and risk scores.

    - A member suggested a working session to explore the possibility of providing impact and likelihood values and finding a way to balance these considerations. A member volunteered his team to provide data for the discussion given that the team is working to explain the impact of a particular vulnerability by using the underlying weakness.
- A member provided an overview of the macro usability updates, which are intended to be some incremental but significant improvements that can be made by the release of CWE 4.17, ideally in the next few weeks.
    - The update process is intended to make small but substantive incremental improvements, such as resolving the wall of text problem. The initiative is also aimed at addressing how individual CWE entries are presented, potentially to include code examples and to simplify how elements are displayed.
    - A member noted that a potential challenges for the usability of SQL injections would be that CWE may not capture multiple variants given existing diagrams. They also recommended adding a link to the NVD for each CWE in the Selected Observed Examples table. A member noted that this is one consideration the team is making and would relate to each particular CWE where applicable.
    - A member shared that visual changes to the table will help to provide clarity and improve readability.
    - In a discussion on changes to the diagrams, a member suggested showing two diagrams side by side, one to demonstrate weaknesses and the other to show neutralization of input before it goes into the sequel query. A member noted that adding information at this stage should serve multiple use cases. A member suggested that this may be a design consideration and that updates to the illustration style could clarify the point.
- A member provided an update on the hardware content for the next release, including three submissions related to hardware, progress on the most important hardware weaknesses list, and ongoing discussions on ranking and data collection.
    - The Hardware SIG reviewed one submission and recommended the submitter lay out a stronger case for why it was a security weakness. A member and team have been working with that submitter to make additional changes that will be brought up to members of the Hardware SIG in the near future.
    - The team has also completed hardware content-related work, such as a discussion of some existing demonstrative examples for some CWEs.
    - A member discussed the progress on the most important hardware weaknesses list, including data collection and the need to curate the data for the updated list. A member also highlighted ongoing discussions on how to

combine data with expert opinions to create a defensible ranking for the most important hardware weaknesses. He also mentioned a submission about inadvertent leaks of cryptographic data through hardware, which has been generalized to include any sensitive information leaks through hardware mechanisms.

- A member also shared that a recent win has been that over 80% of CNAs that had a CVE record published in the past year provided CWEs with their records, showing that there is uptake in the broader community.
- A member introduced the development of the grounded LLM tool to assist with RCM for CVE records. Members who has been working to build out the tool demonstrated the tool's capabilities and discussed future work to improve its accuracy and usability.
    - While updates are still ongoing, especially in the areas of using retrieval augmented generation (RAG) to ground it and providing guardrails to keep the LLM on topic, members have been able to ask the chatbot some questions with success.
    - A member that they will be presenting at VulnCon 2025 on vulnerability RCM with a focus on challenges, solutions, and insights from grounded LLM-based analysis.
    - A member suggested adjusting the temperature of the model to try to reduce variance, which was discussed as part of tuning it. They also recommended identifying which use cases the LLM tool should consider given that CWE mappings may vary in accuracy.

### Open Discussion

- A member shared that there will be updates to the OMG standard that underlies ISO 5.5, which includes 138 serious weaknesses that all now have CWE numbers. They will be hosting a meeting on Thursday, March 20th at the Hyatt Regency in Reston, VA, and anyone who would like to take part in the discussion is welcome to join. The meeting is intended to examine if the current weaknesses are severe enough to stay in the standard, as well as whether there are others that should be included and if the current weaknesses should be modified.
    - The meeting will include a discussion on the formal representation for each of the weaknesses in the standard presented by one of the leads of that work.

## Next CWE Board Meeting

- Wednesday, May 7, 2025, 2:00pm – 3:30pm (EDT)

## Discussion Topics for Future Meetings

- The May 7th meeting will include a working group update session.

- If you have topics for the CWE Board to discuss, please reach out to the CWE Admin.