CWE Board
Meeting Minutes
May 7, 2025

Meeting Attendance

- Attendees:
  ☒Steve M Christey (Guest)
  ☒ Chris Coffin (Guest)
  ☒Bill Curtis
  ☐Chris Eng
  ☒Jason Fung
  ☒ Eric Galinkin (Guest)
  ☐Robin Gandhi
  ☐Jay Gazlay
  ☒Bob Heinemann (Guest)
  ☒Alex Hoole
  ☒Joe Jarzombek
  ☐Jason Lam
  ☒Chris Madden (Guest)
  ☒ Manna Parbati Kumar (Guest)
  ☒ Connor Mullaly (Guest)
  ☒Jason Oberg
  ☐Deana O'Meara
  ☐Kurt Seifried
  ☒Alec J. Summers
  ☐Chris Turner
  ☒Jeremy West

Agenda

- Introduction
- Root Cause Mapping Working Group
- User Experience Working Group
- Hardware SIG
- AI Working Group
- CDR Status Update
- Software Content Goals
- Open Discussion

Action Items

- None

Topics

Introduction

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

Root Cause Mapping Working Group

- The Board was briefed on the status of the Root Cause Mapping working group (RCM WG). The group is reassessing its meeting cadence, considering moving to monthly meetings to maintain engagement. The working group may also implement outreach plans to engage with the wider CNA community. This may include posting previous RCM WG presentations on use cases to YouTube and establishing a public discussion forum on Slack or another platform.
- The working group will continue to engage with a product security engineer at Yahoo who has been supporting the development of the grounded LLM-based tool to help the community with root cause analysis for vulnerabilities.
- A member noted that a presentation was delivered at VulnCon, which will be uploaded to YouTube. Feedback on the presentation was positive, showing an interest in and the relevance of CWE mapping and LLM solutions for CVE enrichment and CWE assignment. They proposed creating a benchmark for LLMs for mapping to CWEs, inspired by discussions with PhD students in cybersecurity. The goal is to finalize participants for the CWE RCM benchmark community collaboration and have a data set, scoring method, and leaderboard by Q1 of 2026.
    - Participants will include representatives from universities, industry, and AI research teams.
    - A member highlighted an existing benchmark created by Rochester University, which covers various aspects including root cause mapping. However, the current benchmark is limited, and the goal is to create a more comprehensive and accurate benchmark.
- A member raised a question about the accuracy of labeling for CVEs and the issue of responses only reflecting positive testing, which is vulnerable and pre-labeled to be correct, noting that permutations of test cases that are not vulnerable should not be labeled. In response, a member noted that in a hallucination where a CWE is not a CWE, part of the benchmark will cover that case. Another member clarified that the benchmark review will analyze vulnerability descriptions, not code. Another

member added that it could improve how CVE records are written as well as precise mapping to correct CWE for someone disclosing a vulnerability. Another member added that the data set would contain an example such as a CVE description and reference content, closely mirroring what was done for the MITRE top 25 mappings.

- A member shared that the applications for the tool extend beyond the current capabilities, noting that it has applications to potentially extend the data set and integrate all hardware CWE mapping activities.
- A member shared that the hardware data set, once finalized and vetted by hardware security, can serve as a data set that will enrich the mapping tool.

User Experience Working Group

- The Board was briefed on the User Experience Working Group (UEWG), noting the group's progress on entry cleanup, understandability, and completeness. The group has been focusing on many macro-level improvements to improve the readability and usability of CWE entries.
    - In the 4.17 release, the group added visual aids to 20 CWE entries. These changes aim to make the content more accessible and easier to understand for users.
- A member mentioned plans to target new members for the UEWG, specifically those with less CWE experience and fresher perspectives on using CWE. The group aims to gather more feedback and improve the user experience further.

Hardware SIG

- The Board was briefed on the Hardware Special Interest Group's (SIG) recent activities, including the addition of 14 new members since the last update. The group now has 158 members, with representation from various companies and academic institutions, including Dell, AMD, Caspian Technologies, and Lenovo.
- The Hardware SIG has met to discuss topics including a presentation of accepted new hardware submissions, a covert channels proposal, system Verilog vs Verilog, usability updates, Hack@DAC, security issues due to hardware design, the most important hardware weaknesses, and memory access related weaknesses.
- Siemens presented a series of ideas about security issues that could arise from hardware design. The group is still processing this work and determining how to handle it.
- The group is currently in the middle of data analysis and expert opinion collection for the most important hardware weaknesses list refresh. The group is conducting a query among members to collect information on what they think the most important weaknesses are. Following that, the group will identify the most common weaknesses and perform a ranking exercise. The bucketing of data and expert opinion gathering will include four scenarios to assess the data. The target completion date for the analysis is July.

    - In response to a question on whether CVEs and relevant CWEs are being reported for the analysis, a member shared that some information is not being fielded, so there would not be a CVE because weaknesses are detected before they are shared.
    - The group has yet to determine if the list of CWE most important hardware weaknesses will be unranked so as not to indicate increase of severity in the list.
    - A member asked whether, given the last list from 2021 and CWE-1277 firmware not updatable, the group is considering the implications between CWEs if firmware is updated but not securely or as an attack vector. Another member noted that if someone has an insecure firmware update process, it would be characterizable by the CWE that makes that update process insecure. When asked if additional guidance should point users who are reporting CWEs to consider associated CWEs, Steve said that information exists in some circumstances, but it may not be as available for hardware. They noted that in 2021, the group finalized the list internally following a systematic investigation of the CWEs that were on the list to fill in gaps. Another member emphasized the importance of warning users about how the top 10 weaknesses may introduce new weaknesses.

AI Working Group

- The Board was briefed on the AI Working Group, which meets every two weeks via two sub-groups. The first covers existing entry modifications, which identifies additional "regular" CWEs commonly found in AI/machine learning products, and the second covers new entries, focusing on the kinds of CWEs that the widespread adoption of AI introduces. The new entries sub-group is also making significant progress on submission for generative AI/machine learning model inference parameters, although they did not meet the CWE 4.17 deadline.
- The overall group also made the first major update to CWE-1039 on adversarial perturbations since its initial publication in March 2018.

CDR Status Update

- It was announced that the CWE Content Development Repository (CDR) has transitioned to a public GitHub repository alongside the CWE 4.17 release, allowing anyone to view current submissions. This move aims to increase transparency and community engagement. The team has not encountered any problematic interactions so far.
- A member discussed common submission problems, including unclear weakness descriptions and submissions being too attack-focused as opposed to discussing the inherent weaknesses that allow attacks to occur. These issues often require extensive back and forth with submitters to resolve. The team is working on improving the submission process to address these common problems. This

includes providing clearer guidelines and feedback to submitters to help them refine their submissions.

- A member provided statistics on the CDR, noting that there are 94 active submissions, 87 of which are open in CDR. For phase change readiness of submissions, 28% are waiting on the CWE team, 24% are waiting on submitter responses, and the final 46% are under consideration for moving to the next phase. The goal is to move submissions through the process more efficiently.
- A member noted that CAPEC work is not happening actively, and currently, it is not part of the sponsor priorities, which indicates there are gaps in CWEs that lack associated CAPECs; however, this appears to be part of a broader problem that is beyond the scope of the working group's activities. Another member suggested that tracking CAPECs may be beneficial for mapping those gaps. Another member noted that not capturing attack pattern information may may be a missed opportunity. A member pointed out that given the existing overlaps in common problem types among CWE entries, it would not be beneficial to add new content that overlaps with existing information, causing redundancies and potentially leading to confusion and greater mapping inaccuracy.

Software Content Goals

- The Board was briefed on the goals for improving software content, including miscellaneous development goals, hierarchical and organizational improvement, and repo-wide completeness initiatives. Miscellaneous development includes finalizing changes from past work such as the ICS/OT SIG and PLT Top 20, updating mapping notes based on real-world RCM, identifying and fixing minor errors and inconsistencies in the repository, and potentially integrating results from CWE-adjacent projects. Hierarchical improvement goals include identifying and adding "intermediate" entries, cleaning and extending Pillar-level entries, and closing important gaps.
- A member also noted that currently, most software content development is driven by community efforts.
- A member suggested looking at the injection-related categories in CWE 20 to consider how to group them better. Steve discussed the concept of neutralization, noting that the current approach lessens the likelihood of reinforcing mistaken assumptions that all injection issues are related to input validation. The work does reflect some chaining relationships between input validation and neutralization and injection issues; however, the software content goals deal with hierarchical changes similar to those in CWE 693, which deals with insecure projection mechanisms that have dozens of child-CWEs.
    - They suggested that it would be beneficial to examine the most commonly misclassified CWEs in the top 25 and whether there is a potential cause for misclassification based on current processes. A member noted that users

may not recognize which CWE is the initial case of an issue, and that they discourage relying on a CWE without determining that it has lower-level children.

- A member pointed out instances leading to buffer overflows when CWEs are exploited. Another member noted that, while helping users understand and navigate chaining relationships could be helpful, it is not in the scope of the current set of goals, adding that there are some gaps in what could be flagged as chaining relationships which have not yet been flagged.
- A member suggested this may present an opportunity to develop a top misclassified CWE list. Steve noted that data is currently available to help teach which CWEs are most commonly misused in mappings. CWE 20 ranks highly among them. As they adjust factors like the mapping notes, they can use the data to help label CWEs.

Open Discussion

- No discussion was held.

Next CWE Board Meeting

- 2 July 2025