CWE Board
Meeting Minutes
September 24, 2025

Meeting Attendance

Attendees:

☐Bill Curtis
☒Chris Eng
☒Jason Fung
☒ Erick Galinkin (Guest)
☒Robin Gandhi
☐ Ganand Ganesh Kini (Guest)
☐Jay Gazlay
☒Alex Hoole
☒Joe Jarzombek
☒ Bob Heinemann

☐Jason Lam
☒ Parbati Manna (Guest)
☒ Connor Mullaly (Guest)
☐Jason Oberg
☐Deana O'Meara
☐Kurt Seifried
☒Alec J. Summers
☐Chris Turner
☐Jeremy West

Agenda

- Introduction
- Working Group Updates
  - AI Working Group
  - Hardware SIG
  - User Experience Working Group
  - Root Cause Mapping Working Group
- Open Discussion

Action Items

- None

Topics

Introduction

- A member welcomed attendees, overviewed the agenda, and introduced members who will brief the status of the ongoing projects. The meeting aimed to facilitate Board feedback on ongoing matters.

AI Working Group

- A member, who chairs the AI Working Group, shared that the group is split into sub-groups. One group is working on new CWE entries that are reported through issues or discussions within the working group, observations of CVEs. The other is working on observation of CVE IDs in applications that have LLM and other AI components integrated into them.

- The working group has developed a backlog in the CDR and has discussed various strategies for members to contribute information that will streamline parts of the process. The group has four CWE entries as observed examples so far.
- Members are also examining existing CWE entries that may have an AI component, which the group may include in either observed or demonstrative examples related to AI or updated to include what the group finds. For example, hidden functionality is a topic the group is considering, including whether "backdooring" or "poisoning" a model should be considered hidden functionality, or it should be considered a new CWE that is a child of hidden functionality.
- A member asked for collaterals that the working group has built that could serve as examples for others to refer to, and a member recommended several CWE entries developed by the working group:
    - 1426 and 1427 that concern generative AI input and output
        - https://cwe.mitre.org/data/definitions/1426.html
        - https://cwe.mitre.org/data/definitions/1427.html
    - There are also issues with commentary in the CDR to advance the discussion:
        - https://cwe.mitre.org/data/definitions/1434.html
    - A member pointed to these as the most meaningful and impactful collateral so far. The group also updated 1039 to be more general than it was:
        - https://cwe.mitre.org/data/definitions/1039.html
- Following a question from a member on the projection of the new contents the group is working toward, a member shared that the working group is developing a submission around the presence of ANSI escape codes in tokenizers as well as a submission on configurations used for model context protocol (MCP) servers.
    - The MCP configurations may be a special case of CWE-77 and CWE-1427, and discussions are ongoing.
- A member raised a point about threats to data security when model distillation is actually model stealing. A member offered to raise the point in the working group, noting that the difference between them is whether permission has been granted.
- Members discussed the potential of data security being compromised for the sake of higher quality reproduction of content. A member considered how this issue can be captured as a weakness.

- A member asked whether there would be variance in this category, and another member shared that the group is taking a flexible approach and trying to remain open to variants that haven't been considered yet.
- A member raised a question about detecting types of weaknesses dynamically in hosted AI chat bots, which are used in creating the top 25 vulnerabilities or weaknesses, for example. This has shown that a large majority are only variants on prompt injection. A member asked whether there should be a base class for prompt injection with variants of it for each specialty. A member advised against trying to delineate against the weakness types because the weakness is ultimately the same. A member raised the point that prompt injection may point to distinct variants that require different testing and remediation, which a member suggested another member take to the AI working group for discussion.

Hardware SIG

- A member provided an update on the Hardware Special Interest Group (SIG). The member and their co-chair shared updates on the group, which has 160 members and added 24 new members since May 2025.
- The group has been discussing memory access-related weaknesses, which involve adapting traditional software memory weaknesses to the hardware view. This is a complex topic with many questions still being worked through. Other topics of discussion include CWE Gaps based on the Most Important Hardware Weaknesses data, presentation of late-stage submissions such as CWE-1429: Missing Security-Relevant Feedback for Unexecuted Operations in Hardware Interface. The Most Important Hardware Weaknesses discussion has spurred the spin off of an ad-hoc working group. The SIG will meet on October 10th where the group will review another late-stage submission to offer feedback.
- Members highlighted the success of the most important hardware weaknesses release. The group used a combination of data from various sources and expert opinions to create a high-quality output. They also discussed the process of incorporating data and expert insights to update the list. The group has concluded and released the updated list.
- A member pointed out that the list is a data-driven approach that highlights the lack of data in certain areas, adding that it is a call to action going back to all vendors to improve data quality so the next round may result in a data-driven approach.
- A member raised a question on access control and needing examples that cover the intersection of hardware and software, citing CWE-1262. A member pointed to similarities in discussions on firmware that may carry over to this domain. A member agreed, citing distinctions between kinds of issues where software,

firmware, and hardware intersect. The member emphasized the benefit of having valid examples of where firmware or software can help, noting that it would depend on the threat model. Other members discussed the role of chaining to capture the weaknesses in the applicable levels. A member noted that there is a formalized concept of chaining in CWE already. Although they focus on software weaknesses, they may be applicable to hardware as well.

User Experience Working Group

- A member delivered an update on the UEWG, highlighting that the co-chair presented on a new initiative at Red Hat aimed at assisting product teams with weakness prioritization and remediation. Red Hat uses SaaS, their operating systems, and some products in combination with their static analysis tools, then use CWE to categorize that to understand how CWE may affect that particular category. This presents a potential use case for CWE.
- A member asked about the use of CWSS, a scoring system to priorities CWEs based on relevance to the environment. A member noted that while there was no discussion on CWSS in the last UEWG and that it is not being actively developed, there may be some applications for its use via AI tools. Another member recommended reviewing CWSS to determine if it could provide a benefit so the group could avoid duplicating services and processes that already exist.
- The UEWG is also developing a CWE survey. The next step is to coordinate with other CWE team members to generate ideas on questions that represent topics from across the community. The CVE survey, which served as the basis for the CWE survey, generated helpful data and feedback, which would also benefit the CWE team to obtain.

Root Cause Mapping Working Group

- A member delivered a presentation on the RCM working group’s activities and goals. The group aims to improve mapping accuracy of vulnerabilities to their root cause weaknesses. The group has been meeting since April 2024 and meets on a monthly schedule.
- The group is working on an LLM tool to help map CWEs to CVEs, which aims to improve mapping across industry. A collaborator from outside the working group has been supporting the development of the tool, creating a proof of concept that, when finalized, would suggest mappings based on CVEs and would include descriptions as well as references. The proof of concept has been used as part of the top 25 outreach for this year. As a next step, the group aims to build the tool into a chatbot for users to ask questions about CVE descriptions that map to CWEs.

- A member shared that the group is looking for two to three volunteers to test the tool, aiming to get early feedback by next month.
- The group is also conducting the CWE BenchMark initiative, which aims to create a benchmark dataset and scoring methodology to test how well an LLM maps CVEs to CWEs. Multiple proposals have been written, and while the Top 25 initiative has slowed activity on the benchmark, the group will reconvene in November to continue developing the dataset.
- The group has also been developing the Top 25 updates based on feedback from CNAs, common questions, and overall progress. The group has also welcomed new members from the CNA community as part of the Top 25 outreach. These include Danfoss, Open Design Alliance, and CrowdStrike.
- The working group has also presented on various mapping examples that the group aims to release as YouTube videos.
- In response to a question from a member on the inclusion of hardware CWEs in the dataset, another member invited members to submit examples to help train the model.
- Members discussed approaches to including CVE descriptions in the training data. Alex also recommended the group discuss CVE fixes, a collection of open-source projects that map pre-imposed patches.
- The group discussed the approach to LLM mapping and where the tool will be hosted. Members suggested hosting the tool as a download that users can host locally. Another member raised the question of batch processing versus a single match at one time, and a member noted that the collaborator has been working to batch process CVE records in testing, as was the case with the 2025 top 25 data.
- A member suggested that a public tool for batch assignment would meet the needs of some community members.

Open Discussion

- A member emphasized that the UEWG should review CWSS as they prioritize CWE, suggesting that a comparison could help maintainers update the CWSS records. Another member noted that the suggestion has been raised before, noting that the resource may be out of date and could use a refresh.
- A member added that he sent an email in July on the recurrence of nine CWEs in the top 25 between 2009 and 2023, which he flagged for discussion. Another member pointed to the release of the stubborn weaknesses list, which may have answered similar questions. He added that multiple weaknesses have appeared in the top 25 repeatedly.

- That member shared that Alex Pinto, the lead researcher for Verizon's DBIR annual publication, may want to partner with CWE in the publication to discuss this and other issues.
- A member raised concerns about AI security, data infrastructure, and the impact of these concerns on CWE records. A member noted that there are certain criteria that will not fit into CWE definitions, adding that speeding up content creation of AI issues likely will not resolve this issue. Members also discussed the roles of hardware and firmware as they impact AI security, with a member advocating for the group to identify the relevant aspects and work towards identifying and working on gaps.

Next CWE Board Meeting

- November 19, 2025