CWE Board
Meeting Minutes
January 15, 2025

Meeting Attendance

- Attendees:
  - ☐Paul Anderson
  - ☒ Steven Christey
  - ☐Chris Co@in
  - ☒Bill Curtis
  - ☒Chris Eng
  - ☐Kate Farris
  - ☒Jason Fung
  - ☒Robin Gandhi
  - ☐Jay Gazley
  - ☒Bob Heinemann
  - ☒Alexander Hoole
  - ☒Joe Jarzombek
  - ☐Jason Lam
  - ☐Parbati Kumar Manna
  - ☐Dave Morse
  - ☐Connor Mullaly
  - ☒Jason Oberg
  - ☐Deana O'Meara
  - ☐Przemyslaw Roguski
  - ☐Kurt Seifried
  - ☒Alec J. Summers
  - ☒Chris Turner
  - ☒Jeremy West

Agenda

- Introduction ○ Update: The Board will meet every other month for an hour and a half.
- Topics ○ CWE 5.0 – Usability Milestone and Future Direction ○ VulnCon Presentations and Board Participation
  - Update on Submitted Topics
  - Discussion of potential additional topics and Board engagement

Topics

CWE 5.0 – Usability Milestone and Future Direction (Alec Summers)

- Milestones to recognize, promote, and emphasize usability improvements ○ Usability has been the driving domain for the past year, and the group has made headway in numerous ways. Finding ways to remove redundant language has been an improvement bringing the group closer to achieving easier usability for CWE.
    - CWE 5.0 features include a new landing page, CWE entry pages, entries default "overview," changes to the color and presentation for type, changes to layouts of complex fields, removing/minimizing IDs in categories/views, and making the CWE website features more apparent. ○ Earlier discussions around what major features went into CWE that would warrant a major version number increase should now consider that, historically, prior to 4.0, version increases accounted for what was in the taxonomy dataset and schema. New entries, such as support for hardware or quality, suggest the prior definition is di@erent from the more recent definition on the CWE site, which is more focused on the taxonomy. Some new schema updates are associated with hardware.
    - Is there a need for a di@erence between versioning of the CWE versus versioning all tools?
        - They are tools as opposed to CWE features. When a taxonomy changes, it impacts the tools, which have to be updated. It may be more usable to create a label that logically groups updates to promote around a set of features that are being released as opposed to the taxonomy.
        - Schema versus content and downstream tooling: There are some downstream tools being relied on the format of the content separate from the schema. That would require advanced notification.
        - Tools built tied to rest APIs would change when the APIs change. Those could be tied to the CWE version number. Format changes may be too infrequent to be the only criteria for CWE version number updates. An accumulation of smaller usability updates should be balanced with large, singular changes.
        - It will also be important to take feedback into account and tailor announcements to changes to the site structure.
        - Establishing CWE 5.0 sets expectations in the community. This means updates should surpass previous expectations and should reflect understandings of motivating factors for and criteria of updates. That message currently is improvements to usability. However, discussion suggested that the enhancements to usability

do not fundamentally change CWE from 4.0 to 5.0. Significant changes to the schema may align better with versioning up. In addition, the purpose of usability improvements—whether to increase the e@iciency of users' work output or merely to make the site easier to navigate—will be weighted di@erently.

- Many of the updates listed are features on the CWE site or server. With that in mind, is there anything limiting CWE from having year, quarter, and minor versioning scheme for the site? Maturity metrics can also help to define versioning updates.
- The group suggested setting milestones around major usability improvements with the caveat that not all changes constitute version changes. The group also discussed postponing naming the CWE as version 5.0. Alternatively, the group is currently at an undetermined 4.xx version. This should still maintain the trajectory of the next release, so it will likely look like a minor release before a full 5.0 release that would break downstream tooling and schema engagement. This would require labeling and storytelling for other tooling like the introduction of the Rust API.
- The group discussed having a tentative date of release. This could align with the conclusion of the refresh of the most important, harder weaknesses, but not necessarily occur at the same time. The goal would be to release good content in succession to keep engagement steady.
- The most important hardware weaknesses list may also need to undergo a refresh. The Hardware SIG is working toward publishing that this year.

- Search / CWE "chatbot" (name forthcoming) ○ The Root Cause Mapping working Group has been partnering with community members to drive work on a chatbot that expands search capabilities.
  - ○ Reporting and disclosing CWEs at the time of disclosure can be a challenge for users to navigate, so to account for feedback, the working group is undertaking a project to develop a chatbot aimed to improve search capabilities. LLMs sometimes hallucinate results, but the working group is developing methods to ground the LLM.
- CDR Public Release ○ It is almost ready for release.
- New entries/contents adjustments
  - ○ New entries and content adjustments are being implemented to reflect a more mature CWE.
- Improve web log management/monitoring ○ These aim to improve understandings of the user experience by reducing friction from initial user

access to where they want to visit, accounting for how many steps are taken for the user to be directed to the desired point.

- The targeted next release is the end of March or early April.
    - This will be the last release of the period of performance, which operates from April to April.

VulnCon Presentations and Board Participation (Alec Summers, Steven Christey)

- CVE/First VulnCon 2025 ○ The inaugural VulnCon focused in detail on vulnerability management. Panel discussions included root cause mapping and gave CWE a platform to speak in detail on the value of RCM. That led to momentum behind pushing to improve products in the PSIRT. Now, there needs to be demand for people to see their improvements. The CVE records should provide the root causes as well. Since the last conference, the has been a significant increase in awareness and adoption of CVE. ○ The program is seeking CWE-related topics again this year. The event will take place April 7-10 in Raleigh, NC. CWE submitted two subjects—RCW and LLM analysis, and the use of "weakness" language. Another topic on problems about CWE and their relevance to the industry is a third paper that will be submitted. Other CVE-related talks will also discuss CWE. ○ The group invited members to propose topics and submit additional topics for discussion.
    - The group recommended using the breaking the language barrier discussion to list the most frequently used cues in those attacks.
    - The group also recommended choosing three vulnerabilities that had broad industry impact in the last 12 months to include in a panel discussion convening key stakeholders including from across government and industry to discuss challenges.
        - For example, Red Hat has many CVEs but would appreciate being included in the discussion of their CVEs. Another topic could include transitioning to memory safe languages and considering what the next CWEs that the community should focus on are.
    - Another suggested topic is to recap e@orts the RCM Working Group has undertaken over the past year as discussion points or best practices in the style of a white paper presentation. This could touch on the purpose behind data collection. This topic is related to the vulnerability RCM with CWE discussion that has already been planned, which will discuss the e@icacy of using a tool and grounded LLM technology to improve mapping. ○ For the VulnCon session on hard problems in CWE, users are being faced with a new technology, and CWE doesn't speak the language that aligns to that technology although it has the same kind of problems. Steven Christey, who

will help deliver the presentation, aims to discuss the RCM challenges in CWE. The session aims to cover problems such as the aspects of CWE's structure that makes it di@icult to add new content. The session will cover broad problems and challenges that reflect issues across the industry itself. The discussion will also consider existing research gaps that need to be addressed.

- Another discussion point noted that other talks on CVEs discuss the measures that CWE has created based on detecting and counting the number of weaknesses in an application. This has helped lead to an international standard for measuring the quality of software and security, reliability, performance, e@iciency, and maintainability. Bill Curtis, who raised the point, may submit a proposal to present on this topic.
- Jason Fung discussed how AI tools are harvesting public information to build their knowledge base, meaning it is critical to ensure these AI engines can generate secure code that they learn from all sorts of repos.
    - Alexander Hoole shared that SAMATE, a large repository that NIST built with the intention of the data being vulnerable, may provide a use case for Jason's point of discussion. The call to action CWE could provide is to have the data owners work with MITRE to link their respective entries and give CWE the dataset, which would ideally include both hardware and software examples.
- **ACTION: Steven will coordinate with Jason via email to discuss overlap between generating secure code with AI tools and Steven's presentation.**
- **ACTION: Alec will share the link for members to submit proposals. Members who want to submit a topic or participate in an existing one should contact Alec Summers.**
- **ACTION: Any member interested in presenting at the AeroTech Conference in May 2025 in Vancouver, especially on the topic of the exploitability of cyber-physical assets and CWE, should contact Joe Jarzombek, who is organizing the cybersecurity track at the event.**

Next CWE Board Meeting

- Wednesday, March 12, 2025, 2:00pm – 3:00pm (EDT)

Discussion Topics for Future Meetings

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