CWE Board
Meeting Minutes
August 28, 2024
CWE Board Only – not for public release

Meeting Attendance

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

Agenda

- Introduction
- Topics
  - Update on the Top 25 Process (Alec)
  - Root Cause Mapping Tool Development (Alec)
  - Recommendations for CWE 5.0 (Alec)
  - Renaming CWE Contributors when organizations change names (Alec)
- Open Discussion
- Review of Action Items
- Closing Remarks

Topics

Update on the Top25 Process

- Top25 is scheduled for publication on October 24th.
- We create it by the data, so CVE records and their accompanying root cause mapping. What are the CWEs associated with the CVE records in the dataset, which historically over the last five years has been the last two calendar years, and looking at those CWEs and how many times they occur and the metric of severity, we create the Top 25 list.
    - What is changing this year is we are trying to federate out the idea of data accuracy. What we've started doing is take our keyword search matches, find ones that we think need manual review within reason, and try and take that potential full data set somewhere between 30,000 to 40,000 CVE records down to something more manageable, where over the course of several months our team can validate and verify, find where things need to be remapped, deal with the NVD, and then generate the list that is accurate and useful.
    - This year we are leveraging the CNA community. We run the same thing, find the CVE records that we think are mismapped, we bucket those up into batches and send them out to the CNAS, requesting that they review them and directing them to the root cause mapping guidance. CNAs have a period of time to review those, get them back to us, and then we can generate the list.
        - These batches have been sent out and we are starting to get notifications back from CNAs saying that the automated remap suggestions work for them. Some members have said they are not going to participate.
    - We have the Root Cause Mapping Working Group (RCMWG) and are already seeing new members join as a result of the request sent to CNAs. There have not been many content questions, but we are seeing some questions about what to do knowing that these are going to be changed. We're encouraging all CNAs to update those CWE mappings in their CVE Records via the CVE CNA container for which they are owners and operators.
- This year will include messaging on how the list itself this year will look different. When you're doing trend analysis, it is important to know the methodology as well as how input provided (or not provided) can affect the data and the list.

Root Cause Mapping Tool Development

- The Root Cause Mapping Working Group is working on an example of using LLMs to improve CWE mapping at scale throughout the ecosystem in terms of a tool. It is a consensus model across three different LLMs that are grounded. They're using the data provided to the LLM to generate a useful outcome. It is not just using the larger LLMs across all subjects. It is being iterated upon in the Root Cause Mapping Working Group, with feedback from partners, and also being informed by some of the remapped accurate mappings from the previous Top25 manual analysis.
- Identifying key user stories for when this could be used, and whether it is something that could be directly incorporated into the CWE program via the website or somewhere else that we can point to directly as guidance for the organizations to set it up themselves.
- There have been a lot of problems in AI around hallucinations with these kinds of things and we are limiting that through grounded capabilities and testing a lot to see what is possible.
- **ACTION: Alec will send out information on information sharing and documentation.**

Recommendation for CWE 5.0

- There will continue to be usability updates across the corpus, including around usability improvements within weaknesses themselves. There will likely be some element of additions to existing weaknesses and the possibility of including new weaknesses. The AI Working Group is working on identifying other gaps that warrant new CWE development. Need to start thinking about the next release in early 2025 (January or February) of CWE 5.0. Would like to solicit recommendations for CWE 5.0 from a usability/content/etc. perspective and the priority things we should try to aim for.
- Talking about maybe simplifying the hierarchy – If something is a weakness, what is a weakness that is belonging in CWE versus being a high-level concept.
- A macro-level CWE website update, not necessarily a new CWE website, but within the constraints of our existing infrastructure, how can we improve the website, aside from the hierarchy itself, to be more useful?
    - Making the contents more usable and how can people navigate to the right entry without a lot of expertise.
- Prevention, detection, and mediation – educating people about the common weaknesses and why it is important to recognize them.
- Improvement with the completeness of the metadata associated with existing CWEs – likelihood and impact values, for example.
- Put more of focus on using CWE to ensure memory safety without switching to a memory switch safe language.
- Listing some prompts that help review code for certain weaknesses, in addition to the regular schema of how CWEs are displayed.
- Are there better download formats for LLM fine tuning? This is a large data set and perhaps making it more AI ready for broader adoption is something to think about.
- What can we do to get organizations to do something with the data and actually do more?
- What warrants branding a major release? How is it different from what we were already doing so why would it not be an updated release under 4.0?
    - This will be a continued conversation as we identify what will be in the release.

Renaming CWE Contributors when organizations change names

- This is a question around individual names but also organizational names, with acquisitions, rebrandings, etc. Contributions on the hardware CWE entries are being listed and attributed.
- Generally, we operate under the policy of keeping things with modifications rather than simply changing things.
- The proposal is to keep the information the same, but adding an update, perhaps in parentheses, stating “formally such and such,” after the new name.
    - Following the convention of formally known as and have the historic list back to the origin. Would be done by request and within reason. Request would be sent to cwe@mitre.org.
    - The original contribution needs to remain. Contributor would need to determine if they wanted to include all historical changes between original and the current or just include original and current.
    - Request that the contributor submit a list of CWEs that have that name associated.

Open Discussion

Review of Action Items

Next CWE Board Meetings

- Wednesday, September 25, 2024, 2:00pm – 3:00pm (EDT)
- Wednesday, October 23, 2024, 2:00pm – 3:00pm (EDT)
- Wednesday, November 20, 2024, 2:00pm – 3:00pm (EDT)
- Wednesday, December 18, 2024, 9:00am – 11:00am (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.