CWE/CAPEC Board Meeting #13

Wednesday, September 20, 2023, from 1:00 PM to 3:00 PM ET

Members in Attendance

Board Members	Organization	Attended
Alec Summers	MITRE (CWE/CAPEC Board Moderator)	X
Alex Hoole	Micro Focus	X
Bill Curtis	Consortium for IT Software Quality (CISQ)	X
Chris Eng	Veracode	X
Chris Levendis	MITRE	
Chris Turner	National Institute of Standards and Technology (NIST)	
Jason Fung	Intel	X
Jason Lam	SANS	
Jason Oberg	Cycuity	X
Jay Gazlay	Cybersecurity and Infrastructure Security Agency (CISA)	X
Jeremy West	Red Hat, Inc.	X
Joe Jarzombek	Synopsys	X
Kurt Seifried	Cloud Security Alliance	
Paul Anderson	GrammaTech	X
Robin Gandhi	University of Nebraska Omaha	X

Agenda

- Welcome (1:00PM)
- CWE's Strategic Vision (1:05 PM)
    - Overview of existing program strategy
    - Discussion: Towards a Multi-year CWE Board Plan (1:30 PM)
- Vulnerability Root Cause Mapping (2:15 PM)
- Update on the CWE GitHub Submissions Repository (2:45 PM)
- Adjourn (3:00PM)

CWE's Strategic Vision (Alec Summers)

- The CWE Program was established in 2006 as an outgrowth of the CVE Program. MITRE produced virtually all CWE content updates and new entries with minimal and inconsistent external engagement, and this limited the ability to execute effectively against the program mission and goals.
- In 2019/2020, the program transitioned to a strategy to engage the CWE stakeholder community. We established the CWE Board (includes industry, government academia), and working groups/SIGs to focus on specific domain areas or issues.
- Early program focus was on content development. Now, we would also like to think about how content is being used by different types of users, and find ways to improve that experience.

- *Comment: Still a lot of vulnerabilities being identified. No corresponding story that says the weaknesses enabling the vulnerabilities could have been avoided; that message is not getting out there.*
- *Comment: I think we need to definitely tie the goals of CWE and CAPEC to securing the software supply chain.*
- Ongoing program evolution includes three elements: effective community engagement, strong corpus of information with technical rigor, and a positive user experience.
- Graphic of the CWE organization and the sources of the contributing community, e.g., industry, government, academia. Shows the broad range of involvement.
- Discussion
    - What do members think about developing a CWE strategy and vision to guide the program over the next couple years? Would provide focus for the board, working groups and SIGs.
    - Summary of comments:
        - It was proposed to have a set of objectives around being more proactive, driving more/broader participation, usability, and quality. Objectives should have clear metrics and be tied to activities in the WGs/SIGs.
        - From a usability standpoint, a challenge is selecting the correct CWE.
        - Incorporate training, research, and automation into the strategy.
        - Strategy won't be finalized today. Will put together a draft using today's comments, and the board can review and finalize off-line.

    - (Further details from the slidedeck note taking):
        - *Often CWE is used "after-the-fact". How can we make CWE more proactive? What can we do to accelerate this from "good known weaknesses" to better products? Rather than just providing information, we need to inspire the community on what to do…*
            - Supply chain concerns – messaging on preventing weaknesses before they become vulnerabilities
        - *Objectives need to be measurable. They must identify progress and end-points of objectives. Objectives should be tied into the efforts going on in the WGs and SIGs*
        - *Drive more adoption of HW CWE; many use CWE as part of the CVE efforts, it is not the same on the HW side*
        - *We need objective(s) related to usability*
        - *We need objective(s) related to content quality (e.g., clean-up/add missing elements throughout the corpus)*
        - **Possible 1-year objectives**
            - *Get CWE to work more elegantly and seamlessly in the context of CVEs and SBOMs (CWE is not used in the context that was intended; "CVE is the most common use of CWE that everyone sees" – this is tied to SBOM mvt) – (perhaps enhancing the use of CWSS?)*

        - Vul mgt – most common exposure to CWE is from CVE
        - Alternative view: Software dev, may only have development to CWE and no/sporadic exposure to CVE; first party code scanning identifies flaws mapped to CWEs before deployment…
    - *Better linkage with CWE and Memory Safety*
    - *ISO 5055 CWEs (free) ☺; CISQ is developing a dependable development certification (~year from now); "can you recognize these weaknesses? Which is the right correction for this weakness?"*
    - *All CWEs should have a CAPEC (e.g., CWE-395);*
        - *CWE is a hierarchical taxonomy, not intended for attack patterns for all of the abstract classes; is there something we can be doing as a community to identify which CWEs should be instantiated? This has an impact on usability and identification of gaps in the corpus;*
        - *Should we have a CWE if there is no corresponding CAPEC? Is there an attack pattern? If the weakness cannot be attacked, is it a vulnerability or is it a valid flaw that's not yet reachable?*
    - *Objective: identify opportunity for creating vignette's / distillations of corpus akin Top 25 for different contexts/domains*
- *Act of choosing the appropriate CWE is the biggest challenge going back 15+ years*
- *1) We need a set of training vendors that turn our information into something that is easier to consume. Someone can practice what we recommend. Someone should be able to internalize mitigations and apply it at their job*
- *2) Research: identified areas where there are opportunities for identification of new ways to mitigate weaknesses.*
- *3) HW CWE got quoted in many publications and conference proceedings. Let's track these*
- *4) Automation… we don't do these by hand. How can we work with our EDA industry in HW industry to develop/use tools…*
- We have indicators of top 25 – this should be a reflection of whether the products are secure or not. Are we seeing these things year-over-year?
    - *Reflecting on Maturity Models… also the idea of vignettes; we've had OWASP Top 10… we've had OWASP ASVs (e.g., Mobile ASVs), no such thing as owasp HW ASVs… built in level 1/2/3 maturity model. When we are looking at CWE Top 25, that is domain independent. If you are working on mobile, ics/ot, etc. primary targets are different…*

- *It needs to be easier to understand a listing of tools that can be used in an academic environment; free tools are available on open source software, but within a SW dev environment, within a classroom for example, its hard to recommend tools that can find CWEs in code that is being developed. Are there tools out there that can be used in an educational environment?*
    - Samate tools are free and available, perhaps vendor tools could contribute to an educational environment for learning how to code

Vulnerability Root Cause Mapping (Alec Summers)

- Weaknesses are the root cause of vulnerabilities. They are often introduced early in product development, but not identified until later when it is more expensive and difficult to deal with.
- The program wants to improve the consistency and accuracy of vulnerability mapping. This will allow trend analysis and provide insight into, for example, weaknesses responsible for the most common or severe vulnerabilities.
- Root cause mapping can be improved through better CVE data quality, increased CWE usability such as new guidance material and mapping notes (this is a new field that has been added to CWE entries), and capability development.
- A new working group is being formed jointly with CWE and CVE to look into ways to improve the effectiveness of root cause mapping, and make it easier. Will target CNAs for their suggestions, and collaborate across the community. Next steps are a meeting in early October with initial interested parties, and recruitment and onboarding of additional members.
- *Comment: A challenge is proprietary code where code is not available to review.*
- *Question: How do we deal with a situation where a product uses or incorporates a third-party component that has the root cause weakness?*
    - Answer: This is an example of a nuance the new working group can consider.

Update on the CWE GitHub Submissions Repository (Alec Summers)

- Program is working to increase transparency into CWE content development and submission status. Also working to make it easier to make third party contributions.
- CWE submission process has not changed.
- Launched Pilot in GitHub on September 12
    - Includes all current submitters and their submissions.
    - Collecting feedback from pilot participants.
- Pilot concludes on October 6
    - Pending the resolution of any identified issues from the pilot, the repository will become open to the public at the earliest opportunity.

    - Community members can see and comment on any existing submission in development.

Final Items (Alec Summers, Jason Fung)

- Alec Summers was nominated by Jason to be a formal member of the CWE Board. Check your email for information. A question session will be scheduled and coordinated by the CVE Secretariat.