CWE Board
Meeting Minutes
September 25, 2024

Meeting Attendance

- Attendees:
  - ☐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
  - ☒Norah Schneider
  - ☐Kurt Seifried
  - ☒Alec J. Summers
  - ☐Chris Turner
  - ☒Jeremy West

Agenda

- Introduction
  - Next meeting will be Working Group updates.
- Topics
  - Shifting the long-term goal of the CWE Program away from standards only outcomes to focus on using weakness data to drive risk mitigation outcomes.
  - Top25 Update
  - Continuing the discussion: Thoughts around CWE 5.0
- Closing Remarks

Topics

Long-Term Goal of CWE Program: From Standards to Risk Mitigation Outcomes (Jeremy West)

- Using program data to identify riskiest components (based on CVE count and associated weaknesses) and sponsoring workshops (engineering led) to propose solutions that either address the weakness directly or through mitigation.
    - This is a very relevant question for many organizations trying to make CWE a key part of their software security engineering parts.
    - **ACTION: Form a subgroup to explore the feasibility and planning of workshops.**
- Need to add additional metadata fields to have a productive discussion with development teams.
    - Add programming languages (ideally with percentages) for CVE Affects – Module. Not all CWEs are applicable to all languages.
    - Also need metadata around what the application does and does not process (e.g., sensitive data).
- Need to discuss how we can ensure accurate data with the right CWEs before engaging developers and engineers.
    - Consider a BSIMM-type survey of how companies are operationalizing CWE data in guiding their own development efforts.
- Is the outreach goal to provide guidance on how to better use CWE itself or better guidance to developers on how to interpret and remediate issues themselves?
    - Looking at how we prevent vulnerabilities from happening and how do we eliminate some of the priority underlying weaknesses.
    - Consider adding a primer on the structure of the taxonomy in a way that people can become more comfortable with the taxonomy.
- Is there anything CWE can do to make their technical descriptions more consumable by the developers?
    - Usability is the CWE Program's primary focus this year, working on micro and macro usability improvements to the website. Descriptions and understandability fall into the macro side. Need to find balance between accuracy and usability, and the context around it, when writing descriptions.
    - Sometimes programmers will misunderstand how the language works because they have some assumptions from other languages or other things, but they don't understand how the underlying mechanism of implementing the runtime and all that works.
        - The way the CWE descriptions are written matter a lot and just simplifying it may cause more misconceptions among programmers about how things are actually working and causing those issues.
        - **ACTION: Discussion about how the program presents and describes weaknesses, to make sure the descriptions are not causing more misconceptions among programmers.**

Top25 Update (Alec Summers)

- Changing methodology to make process more manageable b y doing a one-year look from June 2023 to June 2024, and leveraging the CNA community who have bought in and are more interested in accurate root cause mapping in their records to provide review of the mapping. There are now many CNAs who are providing CWE mappings as a matter of routine within their CVE disclosures.
    - The CWE Program, using automated keyword searches, are identifying batches of CVEs requiring review for the CWE mapping accuracy and sending those batches off to the CNAs that own that CVE. So far have received a number of corrections and continue to receive them daily.

Continuing the Discussion: Thoughts Around CWE 5.0 (Alec Summers)

- The last time we had a major release was when CWE's scope expanded to include hardware (February 2020). Time should not dictate when the program has a major release, but we do need to consider what changes/topics would indicate the need for a major release.
    - **ACTION: Create a slide with the different versions and what the major differences/changes were for each release.**
- Usability schema change does not seem to reach the need for a major release, but there should be a new version number when there is a major change in the backward operability.
    - It seems we're trying to justify a major version and that should probably be the cue to pause and wait.
- Does a release have to tie to content structure, API, etc., or could it target perception/marketing? Perception/marketing would lean on talking about some significant update for that version, so it would be good to have some substantial update that is not included in an incremental version.
- What does CWE want to get out of versioning and are we using the correct versioning scheme to get that?
    - Versioning and minor releases are opportunities for several things deriving from the CWE Program's mission and priorities. Periodic publications representing value becoming realized are important. Also brings momentum and attention, especially for CWE that has a less aware adoption compared to CVE.

Next CWE Board Meetings

- Wednesday, October 23, 2024, 2:00pm – 3:00pm (EDT) – Working Group Updates
- Wednesday, November 20, 2024, 2:00pm – 3:00pm (EDT)
- Wednesday, December 18, 2024, 2:00pm – 3:00pm (EDT)