CWE/CAPEC User Experience Working Group (UEWG)
Wednesday, March 8, 2023

Members in Attendance

Alec J Summers – MITRE
Chris Coffin – MITRE
Francis Murphy – DOI
Przemyslaw Roguski – Red Hat
Steven Christey – MITRE
Matthew Coles – Dell
Rich Piazza – MITRE
Faheem Ahmed – CISA
Tim Wadhwa-Brown – Cisco
Cassie Norcross – DOI
Suzanna Schmeelk – St Johns
Doug Nichols – GE Aerospace
Maldonado Rosado, Shadya Beatriz – Sandia
David B Rothenberg – MITRE
Paul Wortman – Wells Fargo

Agenda

- Purpose
- Housekeeping
- Primary Topics
    - User Stories Update
    - CWE/CAPEC Board Readout for UEWG
    - Discussion: CWE IDs and Hierarchy
    - Discussion: CAPEC Program
- Reminders and Adjourn

Purpose (Alec Summers)

- Mission: Identifying areas where CWE/CAPEC content, rules, guidelines, and best practices must improve to better support stakeholder community, and work collaboratively to fix them.
- Periodic reporting of activities to CWE/CAPEC Board (next quarterly Board meeting TBD Q2-2023).
- Solicit participation from your contacts (Contact: cwe@mitre.org & capec@mitre.org).

Housekeeping (Alec Summers)

- We are working to identify further UEWG opportunities and priorities for FY23.

User Stories (Chris Coffin and Przemyslaw (Rogue) Roguski)

- Received first draft from Milind Kulkarni for the “PSIRT team security bulletins and disclosures” user story. Will continue to work to flesh out the draft.

- Question: Where can we find drafts of the user stories? Link posted to chat.
    - https://drive.google.com/drive/folders/1Po2clv_QfhCL8tPTgwvuosIEMLMWe_dS
- Ideas for user stories and/or personas can be emailed to the team.
- Want to publish user stories in stages out of the cycle of a typical release.

CWE/CAPEC Board Readout for UEWG (Alec Summers)

- Briefing update given to the Board February 14.
- Happy with progress and accomplishments.
- Discussed user personas, harmonizing definitions, content filtering capabilities (pre-defined filters, and soon to be released custom filtering capability to enable different types of users to see data of most interest to them), and ongoing user story development.

Discussion: CWE IDs and Hierarchy (Alec Summers, Przemyslaw Roguski, Chris Coffin)

- This is an ongoing issue around certain elements of user experience.
- CWE overall structure and hierarchy is complex.
- An important use case for the wider community is related to our sister program, CVE. We would like to be able to map a vulnerability (CVE) to its root cause weakness (CWE). Difficult process:
    - CVE does not require CWE mapping in its records. It does require a vulnerability type to be identified, but that doesn't always include a CWE mapping.
    - Identifying root cause is difficult. There is a certain gap in capability throughout the community how to do this, which we can help address through guidance, training, etc.
    - Complex hierarchy structure (pillar down to a class down to a base to a variant).
- How could CWE's hierarchy and structure potentially be changed/simplified to make it easier to navigate and understand, certainly with respect to mapping? Some suggestions made:
    - Stop assigning CWE IDs for high-level classes, categories, and views since these are not weaknesses.
    - Something we've already done is to add mapping notes as an element to particular entries.
    - Use CWE numbering to help show parent-child relationships among weaknesses, e.g., parent is CWE 120, child 120.1, etc.
- Comments and questions
    - Don't see any good reason to have a CWE ID assigned to views and categories.
    - Be careful with the ID system for views. A numeric view ID (e.g., 77) could be interpreted as weakness ID 77. Use different ID structures for different objects to avoid confusion.
    - Be mindful of the infrastructure and code logic that is in place across the program and user community. Significant change won't happen overnight, and the community will need time to adjust.

    - CVE record descriptions should include enough information to help identify or map to the root weakness(es) of the vulnerability. They do not currently.
    - Based on my experience, what is pretty common in CVE descriptions is a focus on the final effect/result of the exploit, and not the root cause weakness.
    - Mistake to think there's a single CWE ID for an issue (vulnerability). Found over years of using this that you need to have a field that allows you to assign multiple IDs with a way to point to the one you think is actionable for the flaw.
    - There has been some discussion about how we could create representational structures that allow for different kinds of chaining style relationships to be recorded.
    - Need a way to record why a particular weakness was selected as the fundamental weakness and not other weaknesses associated with the vulnerability.

Discussion: CAPEC Program

- Program strategy is to increase program adoption and program coverage through effective community engagement.
- Over the last 12 months or so, we've seen limited interest/willingness to contribute content to CAPEC versus CWE, and the summit last February didn't catalyze stakeholder engagement in major way. The conceptual value of CAPEC has not resulted in widespread adoption.
- Minimal expansion of adoption/coverage in strategic focus areas
- Have noticed many small pockets of community interest in different areas and stakeholder groups, but little evidence of broad-based community adoption and willingness to participate.
- One modification submission and two entry submissions since April 2022.
- CAPEC will be a lower priority going forward, and the board is considering options for how best to proceed.
    - CAPEC is not going away.
    - There is discussion about putting a banner on the site about maintenance and development slowing and maybe halting at some point.
    - Possibility of the program going open source for maintenance and development.
    - Possibility that a willing organization may take custodianship of the maintenance and development.
    - There is a stakeholder survey to provide feedback that is open until March 10. Go to any CAPEC page and you will see it at the top. The board is meeting next Friday to review the results.

Reminders and Adjourn

- Next meeting is April 5 at 12pm EDT.