CWE/CAPEC User Experience Working Group (UEWG)

Wednesday, June 28, 2023

Members in Attendance

☒ Andreas Schweiger
☐ Alec Summers (MITRE)
☒ Blaine Wilson (BMO Financial Group)
☒ Chris Coffin (MITRE)
☒ Christopher Sundberg (Woodward, Inc.)
☐ David Maxwell
☐ David Rothenberg (MITRE)
☐ Doug Nichols (GE Aerospace, US)
☒ Erin Alexander (CISA)
☒ Faheem Ahmed (CISA)
☒ Jim Duncan
☐ Kirsten Gantenbein (ExtraHop)
☒ Kris Britton (MITRE)
☒ Matt Coles (Dell)
☐ Paul Wortman
☐ Pippen Wang (Telecom Technology Center)
☒ Prafulla Vyawahare (state of California)
☐ Przemyslaw (Rogue) Roguski (Red Hat)
☒ Rich Piazza (MITRE)
☒ Remy Stolworthy (INL)
☒ Steve Christey Coley (MITRE)

Agenda

- Purpose
- Housekeeping
- Primary Topics
  - CWE Views
  - CWE Tips and Tricks
- Reminders and Adjourn

Purpose

- 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 Q3 2023).
- Please solicit participation from your contacts (Contact: cwe@mitre.org & capec@mitre.org).

Housekeeping

- UEWG meeting frequency has changed; they are now set to occur on the last Wednesday of the month, instead of every four weeks.
- Working to identify further UEWG opportunities and priorities for FY23. Any suggestions are welcome.

CWE Views (Chris Coffin)

- A CWE view is a predefined perspective (or representation), from which a user might look at a particular weakness. It is intended to help users understand CWE basics.
- Views also help make navigating the CWE list more manageable. For example, it can help narrow down the list to those specific to certain technologies or languages, or to those specific to a certain audience (e.g., software developer or security researcher).
- Views can be flat or hierarchical, for example:
  - CWEs on the Top 25 list are flat, so they have no tree structure.
  - CWE-1000 is a view that covers all CWEs, so it has a deep tree structure.
  - CWE-1003 is a subset of 130 CWEs most commonly mapped by CVEs.
- There are currently 48 views in version 4.11. This is the link to the views on the CWE website. Also have PDFs that provide a graphical representation of the views.
- Members were asked to provide input to the program about additional views to add.
  - A request was made to add a new view for security architects around vulnerabilities in input validation.
  - Maybe add a view for security requirements, and a view into the taxonomies referenced in some CWEs as mitigations.

CWE Tips and Tricks (Jim Duncan)

- Learning CWE takes time, and using that knowledge to help others learn takes more time.
- Understand your audience. When sharing information about weaknesses identified in your own vendor products (or third party add-ons) with executives and other decision makers, do not deluge them with minutia about what their coders are doing. Give them the high level view. For example, don’t mention buffer overflow as the issue; instead, mention the denial of service resulting from the overflow. That’s what they would be interested in.
- The idea of assigning a single weakness to an issue (vulnerability) is flawed. Weakness assignment should be a list and we need better tools for walking through the variety of items in CWE to make it easier for people to identify the possible weaknesses leading to a vulnerability. Also, we need to make it easier for users to improve the list by elevating or lowering the importance of weaknesses.
- Time to start paying attention to weaknesses associated with AI/ML.
- Take care with CVE entries/mappings; can't tell you the number of times they have arbitrarily been studying something that affected a crypto algorithm and labeled it with cryptographic issues. Comments:
  - CVEs identified as a map to a weakness(es) are vetted first.

    - Been working pretty closely with the NIST NVD team on improving the quality of their mappings. Quality of mappings is improving.

Open Discussion

Out of time.

Reminders and Adjourn

- Next meeting is July 26 at 12pm EDT.
- Questions of thoughts? Contact CWE@mitre.org or CAPEC@mitre.org.