CWE/CAPEC User Experience Working Group (UEWG)

Wednesday, July 26, 2023

Members in Attendance

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

Agenda

- Purpose
- Housekeeping
- Primary Topics
  - New to CWE Examples
  - User Stories Updates
  - Open Discussion
- 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 network (contact: cwe@mitre.org & capec@mitre.org).

Housekeeping

- UEWG meeting frequency has changed; they now occur on the last Wednesday of the month.
- Working to identify further UEWG opportunities and priorities for FY23. Input from members is welcome.

New to CWE Examples (Chris Coffin)

- Received feedback on the New to CWE page asking for more examples, and specifically how a CWE relates to other CWEs.
- Select high quality CWEs that are easy to understand for someone new to the program. An idea mentioned was to look at the Top 25 list as a source of candidate examples.
- After discussion with some team members, a list of proposed new examples include: CWEs 88, 27, 787, and 287 (see slides for details.
- Comment: would be useful to have some examples that show the value of collecting things (i.e., related CWEs) together. So, for example, if you have memory management in general, also include the out of bounds. You can be very specific or somewhat general when looking at the collections of weaknesses.
    - Be careful with this. Make sure you can make a meaningful collection (i.e., well versed enough with CWE).

User Stories Updates (Chris Coffin)

- We have two previously-identified personas that do not have a user story yet, i.e., security analyst/researcher, and educator. Looking for help on these.
- Also looking for new ideas: user description, story, and benefit.

Open Discussion

- Will push for preparation and presentation at an upcoming meeting of a deep dive into how Red Hat is using CWE.
- There is another view (CWE-1400) that is for categorizing CWEs into approximately 22 categories. Has not been publicized much. Could be used similarly to 699.
- A member mentioned that he is reading a guide to automating vulnerability participation using SSVC decision trees. Could this be useful to the CWE program and are other members aware of the guide?
    - Might have more applicability to the CVE Program.
- Question: Has any progress been made on the disposition of CAPEC repository and management?
    - The site itself is not going to go away, but the site isn't actively being maintained. There is ongoing community content development. An open source option is not drawing interest from the sponsor or copyright owners.

- A member presented on some recent work he’s done with risk ratings and risk rating models. Also presented on work from a few years ago that mapped the effectiveness of threats against specific controls, to help steer his team toward appropriate controls, and not simply rely on CAPTCHA. The tool requires a lot of maintenance, and the member would like to hand it off to the CWE Program. Cannot be shared with the group, since it’s been flagged as intellectual property. Will try to get it declassified so can be shared for further member review.
- A topic for a future meeting could be how to group CWEs in the most effective way. Include presentation of the many different ways and categories we have now, and discussion about what works, what doesn’t, and what could be done differently.

Reminders and Adjourn

- Next meeting is August 30 at 12pm EDT (may be rescheduled due to Labor Day holiday).
- Questions of thoughts? Contact CWE@mitre.org or CAPEC@mitre.org.