# CWE/CAPEC User Experience Working Group (UEWG)

## Wednesday, May 31, 2023

### Members in Attendance

☐ Andreas Schweiger
☒ Alec Summers (MITRE)
☒ 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)
☒ Przemyslaw (Rogue) Roguski (Red Hat)
☐ Rich Piazza (MITRE)
☒ Steve Christey Coley (MITRE)

### Agenda

- Purpose
- Housekeeping
- Primary Topics
  - CWE Video Tips Series
  - New to CWE
  - CWE Naming and Vulnerability Mapping
  - 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 scheduled for June 2).
- Solicit participation from your contacts (Contact: cwe@mitre.org & capec@mitre.org).

**Housekeeping**

- Meeting frequency is currently every four weeks on Wednesday. We're thinking about changing it to once a month (last Wednesday of the month). There were no objections in the meeting. Will send out email communication to the entire UEWG list to determine if there are objections from others.
- Continuing to identify new UEWG opportunities and priorities for FY23.

**CWE Video Tips Series (Chris Coffin and Przemyslaw Roguski)**

- Initiative to create short videos (about five minutes) with guidance on how to perform various tasks on the CWE web site, and walk the viewer through certain features of CWE and use cases. Not started yet.
- Some possible topic ideas have been identified, but we're looking for additional topics and priority suggestions from the group.
- Comment:
  - A UEWG member mentioned a CWE presentation that was given at the FIRST conference in 2018 about common weaknesses and tips/tricks section. It could contain useful ideas for the video tips series.

**New to CWE (Chris Coffin and Przemyslaw Roguski)**

- As of the last release, the CWE web site has a New to CWE section. This is designed to help casual or new users understand the basics of CWE.
- For new users, we're also trying to put together some good content and deliver it in more digestible/small chunks.
- Feedback has been received suggesting that other CWE examples be added (in addition to CWE 798 – Use of Hard Coded Credentials).
- Any thoughts about new content and CWE examples are welcome. Also, should content be aligned with the topics covered in the proposed video tips series?
- Comments:
  - Add content that practitioner can use to provide meaningful information to decision makers. Don't want VPs and such having to digest detailed CWE data.
  - Leverage the CVE Program in content/messaging (each vulnerability is an instance of a certain type of weakness).
  - For new examples, consider the top 25 and those that are language-independent.
  - Don't make it a wall of text. Have example files to download. Example videos.

**CWE Naming and Vulnerability Mapping**

- Are there changes to CWE naming that can make it easier for the community to map a vulnerability to its root cause weakness? The current structure is difficult to understand.
- Some users are mapping vulnerabilities to CWE categories/views and not individual weaknesses.

- CVE has grown and is accepted as the de facto standard for defining publicly disclosed vulnerabilities. But we also see that users are making the same mistakes as they map to root cause weaknesses.
- What can we do? What can we emphasize? What can we fund to address this issue?
- Comment:
  - People who generally are disclosing the vulnerability are best positioned to provide information about root weakness(es), but they're not always incentivized to do so in the right way. CNAs and researchers have said they don’t know which hierarchy level to map to.
- An option for consideration is to eliminate CWE IDs from Categories and only have IDs for weaknesses that are mappable root causes.
- Comment:
  - Closed source vendors who provide vulnerability information may not be incentivized to report the root cause, since they’re the ones who will fix it.
- Discussion about a possible terminology change from “root cause” to something that sounds less definitive (implies one cause only). Options mentioned: fundamental cause, nexus, tipping point, actionable cause. A counterpoint mentioned was the program has been moving toward “root cause” because it is a commonly used term that more people can relate to.
- Comment:
  - Could be helpful to reference a CVE(s) within the CWE record. Show examples of pain points (vulnerabilities) happening due to the weakness.

**Open Discussion**

Out of time.

**Reminders and Adjourn**

- Next meeting is June 28 at 12pm EDT. This reflects the meeting schedule change from every four weeks to once per month.
- Questions of thoughts? Contact CWE@mitre.org or CAPEC@mitre.org.