CWE/CAPEC User Experience Working Group (UEWG)
Wednesday, August 30, 2023

Members in Attendance

Faheem Ahmed – CISA
Aliasghar Arab - Nuro
Jill Babin - CISA
Abhi Balakrishnan - Kroll
Kris Britton – MITRE
Steve Christey Coley – MITRE
Chris Coffin – MITRE
Matthew Coles – Dell
Jim Duncan
Jonathan Dutson - Microsoft
Pavan Gudimetta - MITRE
John Keane
Milind Kulkarni - Ericsson
Kent Landfield - Trellix
David Maxwell - BlueCat Networks
Mark Muha - NASA
Vivek Nair - Microsoft
Lisa Olson - Microsoft
Rich Piazza – MITRE
Gerald Rigdon - Boston Scientific Corporation
David Rothenberg - MITRE
Alec Summers - MITRE
Christopher Sundberg – Woodward, Inc.
Prafulla Vyawahare - State of California
Blaine Wilson - BMO Financial Group
Paul Wortman – Wells Fargo

Agenda

- Purpose
- Housekeeping
- Primary Topics
    - CWE Element/Information Presentation
    - Grouping CWEs
    - CSV Download Colon Issue
    - 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.
- The CWE Program is continuously seeking feedback on UEWG activities and priorities during these sessions or via email: cwe@mitre.org.

CWE Element/Information Presentation (Chris Coffin)

- What elements should be presented first to a user looking at/for a CWE, and in what format? Currently, it's a wall of text.
- Custom filters were a step to help with this, allowing users to configure what they see and what might be most applicable to them. But should there be a default view of CWE elements that gives just the right amount of information and the right ordering of those elements? Are there diagrams or graphics that might better help understand the weakness information.
- An example graphical representation of an initial CWE view was shown (see meeting slides). It helps someone quickly see what a CWE might entail. Question to the group whether this would help break up the wall of text and help someone more quickly consume CWE information. Other questions to consider:
    - Who is the audience (new, experienced, of all users)?
    - What elements are most important to those users?
    - Should the program investigate or create a graphical presentation of a CWE?
- Possible activities going forward: volunteer to create a new CWE entry page that improves CWE understanding; and on the program side, propose some ideas for the next meeting. Reactions:
    - Don't use 'wall of text' – negative. Also, need consistent summary information at the top of each CWE page.
    - Create views based on use cases that people are using.
    - User stories may overlap for different types of users/personas
- Next steps: One WG member offered to mockup a new design for a top level weakness and its associated info. The CWE program will also come up with some ideas on potential CWE landing pages to show at the next meeting.

Grouping CWEs (Alec Summers)

- There are over 900 CWE entries in the corpus, and they are grouped in different ways to support different domain areas and different types of users.

- Grouping methods include Views, Categories, and Overall Hierarchy (see meeting slides). Are the groupings effective, and is there a different way to do the groupings to bring better value?
- Program questions to group:
    - Different groupings for new/casual users versus experienced users?
    - Can existing views be presented more effectively, more easily discoverable?
    - Include links to groupings in user stories?
    - Are there additional groupings we're missing? Are there too many?
- Question: Are there demonstrative examples for all CWEs? Examples are helpful for orientation and new users. Answer: Not currently, but the hope/plan is for every weakness to have at least one example, eventually. If you have example ideas, send them to the program.
- Question: Under the category of software, is there more granularity to identify particular environments and domains like embedded systems? Answer: the corpus uses a concept of hierarchy of entries, from general to specific, and is not complete. Program is always looking for new weakness entries to help improve granularity and coverage.
- Comment: It'd be way cool to have a monthly blog post that talks about an interesting CWE. Also, a 10 question quiz a company could use to see what people know about CWE (maybe offer some prize). Another idea would be to highlight a group of interesting non-technical CWEs to include CWEs such as CWE-655 Insufficient Psychological Acceptability.
- A member will share with the group later in the Fall a presentation about mapping of security weaknesses to technical weaknesses.

CSV Download Colon Issue (David Rothenberg)

- A double colon is used to separate csv fields/columns data, while a single colon is used to separate multi-value data within fields/columns
- The Observed Examples field contains Reference and link data that includes a URL in some cases (colon within "http://...")
- Should a note be added to the download data that warns the user of this, or should we look into an alternative separator?
- Example taken from CWE - CWE-41: Improper Resolution of Path Equivalence (4.12) (mitre.org)
    - ::REFERENCE:CVE-2000-1114:DESCRIPTION:Source code disclosure using trailing dot:LINK:https://www.cve.org/CVERecord?id=CVE-2000-1114::REFERENCE:CVE-2002-1986:DESCRIPTION:Source code disclosure using trailing

Open Discussion

- None

Reminders and Adjourn

- Next meeting is September 27 at 12pm EDT (may be rescheduled due to Labor Day holiday).
- Questions of thoughts? Contact CWE@mitre.org or CAPEC@mitre.org.