CWE/CAPEC User Experience Working Group (UEWG)

Wednesday, November 29, 2023

Members in Attendance

Faheem Ahmed – CISA
Abhi Balakrishnan – Kroll
Chris Coffin – MITRE
Matthew Coles – Dell
Matthew DiVisconte – California Department of Transportation (Caltrans)
Jonathan Dutson – Microsoft
Farbod Foomany – Security Compass
Art Manion – Analygence
David Maxwell – BlueCat Networks
Mark Muha – NASA
Vivek Nair – Microsoft
Doug Nichols – GE Aerospace
Lisa Olson – Microsoft
Rae Powers – California Department of Transportation (Caltrans)
Gerald Rigdon – Boston Scientific Corporation
Przemyslaw (Rogue) Roguski – Red Hat
Sonal Shrivastava – Microsoft
Alec Summers – MITRE
Katherine Taylor-Jewell – California Department of Transportation (Caltrans)
Blaine Wilson – BMO Financial Group
Paul Wortman – Wells Fargo

Agenda

- Purpose
- Housekeeping
- Primary Topics
  - Data Mining Mitre.org Projects (Member presentation)
  - CVE –> CWE Root Cause Mapping
- 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 Board (next quarterly Board meeting TBD Q4 - 2023).
- Please solicit participation from your network (contact: cwe@mitre.org & capec@mitre.org).

Housekeeping

- CWE UEWG December Meeting
    - The meeting currently set for 12/27 is being brought forward a week to 12/20.
    - Updated invitation to will be sent after this meeting.
    - The CWE Program is continuously seeking feedback on UEWG activities and priorities during these sessions or via email: cwe@mitre.org.

Data Mining MITRE.org Projects (Blaine Wilson)

- Refer to meeting slides.

CVE to CWE Root Cause Mapping (Alec Summers)

- Root cause mapping (RCM) identifies the underlying cause (weakness) for a disclosed vulnerability. A majority of CNAs do not provide the mapping, and in cases where they do, they often select a broad weakness since it's easier.
- The new CVE record data format provides an easy way to identify the mapping, and more CNA participation identifying the mapping is needed. A centralized mapping solution would be expensive and difficult to scale.
- Reasons to provide accurate mapping: (1) trend analysis, e.g., ability to identify weaknesses as the cause of repeated types of mistakes, (2) illuminates where investments, policy, and practices can address the weaknesses responsible for product vulnerabilities.
- Mapping guidance is on the CWE web site, and includes quick tips and examples, and a cheat sheet of common terms.
- Some methods to help with mapping include a keyword search method to help find CWEs of interest, and the View-1003 method (and other views) that are useful for navigating to and finding different kinds of weaknesses.
- The program also has Relationship Graph Visualizations in downloadable PDF format that can be helpful in mapping.
- There is a new RCM working group (not operated by CVE/CWE) that consists of a set of partners within the CVE and CWE community. It is expected to grow and open up to the wider public in January 2024. The group is bringing together the community under a shared goal and a shared value proposition for trying to drive better root cause mapping throughout the ecosystem.
- Question: For the RCM working group, is there a general purpose tool they've all used that could help with mapping? Answer: No, but the program is thinking about how a tool might be developed and used, e.g., AI-capability, graphical navigation tool (similar to ATTACK Navigator).

Reminders and Adjourn

- Next meeting is December 20 at 12pm EST.
- Questions of thoughts? Contact CWE@mitre.org or CAPEC@mitre.org.