CWE User Experience Working Group (UEWG)
Wednesday, February 28, 2024

Members in Attendance

Faheem Ahmed – CISA
Abhi Balakrishnan – Kroll
Steve Christey Coley – MITRE
Chris Coffin – MITRE
Matthew DiVisconte – California Department of Transportation (Caltrans)
Jim Duncan
Jonathan Dutson – Microsoft
Farbod Foomany – Security Compass
Jonathan Hood – U.S. Army
John Keane
Milind Kulkarni – Ericsson
Lisa Olson – Microsoft
Rich Piazza – MITRE
Rae Powers – California Department of Transportation (Caltrans)
Przemyslaw (Rogue) Roguski – Red Hat
Kyle Rudnitski – CISA
Alec Summers – MITRE
Christopher Sundberg – Woodward, Inc.
Umberto Vizcaino – Merysol Security
Blaine Wilson – BMO Financial Group
Paul Wortman – Wells Fargo

Agenda

- Purpose
- Housekeeping
- Primary Topics
    - Prioritizing Corpus User Experience Modifications
    - Software Licensing Discussion (Continued)
- Reminders and Adjourn

Purpose

- Mission: Identifying areas where CWE 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 Q1-2024
- Please solicit participation from your network (contact: cwe@mitre.org)

Housekeeping

- CWE UEWG March Meeting is cancelled due to VulnCon 2024 happening the same week
- CWE UEWG April Meeting

    - The next regularly scheduled meeting is Wednesday, April 24.
- The CWE Program is continuously seeking feedback on UEWG activities and priorities during these sessions or via email: cwe@mitre.org
- Alec Summers from MITRE and Przemyslaw Roguski (Rogue) from Red Hat will both be presenting at VulnCon 2024

Prioritizing Corpus User Experience Modifications (Chris Coffin and Alec Summers)

- User Experience Working Group was established in response to negative feedback related to CWE's usability
- UEWG has accomplished much in response (e.g., submission guidelines, mapping guidance, "New to CWE?" launch, weakness filtering)
- We must now begin to address usability and understandability in further ways throughout the corpus structure and down to individual weakness language
- Understandability: revising all entries for simpler language; remove redundancy
- Simplifying descriptions/extended descriptions to leverage other elements appropriately
    - E.g., removing example instance, impacts, etc. language from descriptions
    - Only having one description written in concise, accurate language focusing on the weakness
- Completeness: ensuring all entries have basic required elements populated
- Visualizations: adding to entries to explain topics visually (leverage Abhi's top25 examples, build from there)
- A side-by-side example was provided to show how a CWE could be revised for improved usability
- Member comment: Can CWE entries be clarified to state how the entry might be used for root cause mapping purposes or for mapping to ISO 62443
- Plans and strategy for corpus user experience modifications will be developed and shared in future UEWG meetings

Software Licensing Discussion (Continued) (Przemyslaw Roguski and Jonathan Hood)

- Since November, a resurrection of debate around SW licensing issues being in/out of CWE scope on the CWE-Research email listserv
- In 2018, it was determined that "improper licensing" was outside of CWE's scope
    - Rationale: Impact to software and its usage not through the technical exploitation of a software security weakness in architecture, design, or code. Rather, it is through policy/programmatic exploitation.
    - Availability concern comparable with supply chain issues where one disrupts a supplier to stop/limit a product from being delivered, and hence make it not available
- Recent arguments are varied:
    - Pro: Misusing SW licenses can negatively affect maintainability, availability
    - Against: Invalid/Improper licenses cannot lead to a vulnerability
    - Pro: CWE absorbed CQE content ~2018; improper licensing is a code quality issue

    - Against: Licensing issues are not a property of SW, but of the society and economy around the SW
- Member comment: CWE weaknesses are created to discuss weaknesses, not vulnerabilities. It should NOT be required that a CWE weakness lead to a vulnerability for it to be in scope of the CWE Program. A requirement such as this would severely limit the CWE Program
- Some UEWG members feel that Software licensing issues could be in scope and receive a CWE while others do not. It is a fairly even split and will require additional community engagement and discussion
- Member comment: I am on the opinion side of believing that this can be exploited in nonstandard ways to affect the availability, and therefore does have a technical exploit path for the definition of a vulnerability
- Member comment: CWE's currently exist for inaccurate comments, 1116 spelling formatting, 1078 things that are bad coding practices that don't lead to an immediate vulnerability, but do affect the availability and maintainability of software (Steve from MITRE pointed out that these CWEs originated from a quality enumeration effort and there are questions around whether they should remain in the CWE corpus)

Reminders and Adjourn

- Next meeting is April 24 at 12pm EST.
- Questions or thoughts? Contact CWE@mitre.org.