CWE User Experience Working Group (UEWG)
Wednesday, January 31, 2024

Members in Attendance

Abhi Balakrishnan – Kroll
Steve Christey Coley – MITRE
Chris Coffin – MITRE
Matthew Coles – Dell
Matthew DiVisconte – California Department of Transportation (Caltrans)
Jim Duncan
Jonathan Dutson – Microsoft
Pavan Gudimetta – MITRE
Jonathan Hood – U.S. Army
Mark Muha – NASA
Vivek Nair – Microsoft
Lisa Olson – Microsoft
Rich Piazza – MITRE
Rae Powers – California Department of Transportation (Caltrans)
Przemyslaw (Rogue) Roguski – Red Hat
Remy Stolworthy – INL
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
    - New to CWE Updates
    - Software Licensing Discussion
- 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 February Meeting
    - The next regularly scheduled meeting is Wednesday, February 28.

- The CWE Program is continuously seeking feedback on UEWG activities and priorities during these sessions or via email: cwe@mitre.org

New to CWE Updates (Chris Coffin)

- New to CWE is a short and easy to understand introduction to CWE for new and casual viewers of the CWE web site. An idea is to add more examples (currently only CWE-798 is shown) that are easy to understand (e.g., 434, 287), or have good demonstrative or observed examples.
- Member comment: Use an example CWE to show where it fits in the hierarchy, and its relationship with other CWEs in a hierarchy.
- Member comment: We have to assume some knowledge on the part of the new or casual viewer, but we are not using complex CWEs with a lot of terminology that will require a lot of work for the viewer to understand.
- Member comment: There was a possibility of adding a new Persona, or a view of some type, for non-technical users. There would be a cost to do this; is the cost/benefit worth it?
- Member comment: A member noted the use of a risk rating system that includes really technical documentation, but it also includes a simple statement of impact for broader understanding. We could adopt something like that.
- CWE descriptions could be simplified while still maintaining accuracy.
- The Rest API has been released to the API working group. It is in the process of testing, for both functionality and operations. If interested, members can join the Rest API working group.
- CWE is considering adding new documents to the New to CWE series, building on initial topics. Two ideas are to explain CWE views and categories, and a simple document on how to navigate CWE.
- A draft of the New to CWE – Views document has already been created and will be shared with the UEWG once it is closer to completion.

Software Licensing Discussion (Przemyslaw Roguski, Jonathan Hood)

- There has been recent debate on the CWE Researcher email listserv about adding software licensing issues to the CWE scope (this was determined to be out of scope in 2018). These issues are going to become more common and visible, so it's something the program needs to consider.
- If you are not on the CWE-Research mailing list, contact us at cwe@mitre.org and we'll add you. The thread on licensing is public archived here: https://www.mail-archive.com/cwe-research-list@mitre.org/msg00096.html.
- An open question is how to address software licensing. Extend the scope of the program and define a new group of weaknesses related to licensing issues? Or maybe it would be better to create a new program to only focus on licensing issues?
- An example was provided where gaps were found in nine reports on cybersecurity enumeration problems. In these cases, there were no CWE mappings, so it wasn't in the

contract language to fix. Of the nine reports, there were several different types of licensing violations that didn't have a CWE to map to. More info below:

- Jonathan Hood meeting chat:

  In the past 4 years, we have delivered 9 reports that listed software weaknesses in using disallowed code, mostly in the realm of coding in a way that violates licenses. These 9 issues can be described generally as follows:
  • 2 general open source violations (the classics that we're all familiar with)
  • 1 situation where an STTR was awarded to a university, and the university delivered a project with a dependency that was only licensed for educators and students for free. This turned a $200k STTR into a $2M struggle when a prime integrator had to stop the availability of a major system to address the issue. They were instructed to integrate software, and when they did so, had a finding that cost them $2M to integrate it legally.
  • 2 situations where the developer maliciously copyrighted and licensed code so that they could sue if they were ever taken off of the project
  • 1 DFARS violation that I can't elaborate on here in a fully unclassified way.
  • 1 issue of using licensed abandonware (the commercial author has died and did not will the copyright to any particular holder)
  • 2 commercial software license violations (mostly expired distribution license)

  In a discussion with Rogue, the idea of creating something outside of the CWEs was proposed. I pointed out that these issues meet the definitions of the CQEs, but it was determined in 2017 to incorporate the things that fall under the CQEs into the CWEs. These are generally reflected as the Security portion of the CISQ standards (https://www.it-cisq.org/standards/code-quality-standards/). It was also brought up that this does not meet the definition of "vulnerability" that CWEs are using.

  In every part of our Software Assurance report, we are able to (at least loosely) categorize all the things that developers do with software that affect confidentiality, integrity, and/or availability against CWEs. This is consistent with the guidance for establishing contract language around categorizing these types of software weaknesses using CWEs and codifying it in contracts (https://rt.cto.mil/wp-content/uploads/2019/06/Incorporating-SwA-Contracts-2017-11-15.pdf). We have been unable to use CWEs to categorize the cybersecurity impact of these coding errors. It would be helpful if these types of issues can, even at a high level, be categorized as the software weaknesses they are and enumerated with the CWEs.

- One of the things to think about with respect to CWE scope is determining where the boundaries for inclusion/exclusion are. Human weaknesses, for example, have never been included although they can lead to a vulnerability.

- We're moving more and more and faster and faster to a world in which everything is software licensed on the fly and the enforcement mechanisms become essential. We should periodically reevaluate whether this is something to be considered or not.
- Jon Hood will be invited to future UEWG meetings.

Reminders and Adjourn

- Next meeting is February 28 at 12pm EST.
- Questions or thoughts? Contact CWE@mitre.org.