CWE/CAPEC User Experience Working Group (UEWG)
Wednesday, October 25, 2023

Members in Attendance

Faheem Ahmed – CISA
Erin Alexander – CISA
Steve Christey Coley – MITRE
Chris Coffin – MITRE
Matthew Coles – Dell
John Keane
David Maxwell – BlueCat Networks
Lisa Olson – Microsoft
Rich Piazza – MITRE
Przemyslaw (Rogue) Roguski – Red Hat
Alec Summers – MITRE
Prafulla Vyawahare – State of California
Blaine Wilson – BMO Financial Group

Agenda

- Purpose
- Housekeeping
- Primary Topics
    - Red Hat CWE Blog (Co-chair presentation)
    - Technical Weaknesses (Member presentation)
    - 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 Board (next quarterly Board meeting TBD Q4 - 2023).
- Please solicit participation from your network (contact: cwe@mitre.org & capec@mitre.org).

Housekeeping

- Meetings have been changed and are now set to occur on the last Wednesday of the month. The correct/updated meeting invitation is from Chris Coffin. If you have one an older one from Alec Summers on your calendar, delete it.
- The CWE Program is continuously seeking feedback on UEWG activities and priorities during these sessions or via email: cwe@mitre.org.

Red Hat CWE Blog (Rogue Przemyslaw)

- Red Hat published two blog posts: "Red Hat's CWE journey" and "Weakness risk-patterns: A Red Hat way to identify poor software practices in the secure development lifecycle."
- Purpose of the two blogs was to provide an overview of the Red Hat CWE experience, and describe how CWE is used as part of Red Hat's risk pattern assessment.
- We want to increase knowledge of how CWE can be used in daily security work, improve understanding of what a weakness is, and improve understanding of weaknesses versus vulnerabilities.
- Red Hat started using CWE in 2012, and began to do analysis and publish results in a yearly risk report. Used custom groupings until 2022. From the beginning of 2022, our default CWE coverage has been based on the CWE-699 Software Development view. This allows us to more accurately assign a weakness to a vulnerability, or a group of weaknesses that leads to the vulnerability.
- Working to improve CWE assignments to CVEs. Have created a new Root Cause Mapping (RCM) working group.

Technical Weaknesses (John Keane)

- DAST and SAST tools find security issues that never should have been in the code in the first place. Should be used continuously in the build pipeline to find security issues before they are a problem in production.
- The mobile application security verification standard came out, and it was in that standard where they introduced code quality, with emphasis on fixing mistakes before they get into production.
- The concept of buffer overflows was understood in the early 1970s as a technical error (it may cause a system to crash, but there wasn't consideration about security implications). The earliest documented hostile exploitation of a buffer overflow was in 1988. Don't think we have 16 years anymore to wait and see if a weakness presents a security concern.
- Recognized as early as 2016 that there is a large set of quality problems not yet covered by CWE. In 2016, 60% of security weaknesses were directly attributable to quality weaknesses. In 2022, it appears that is now 85%.
- A big surprise with the FORTIFY was it showed significant overlap between safety and availability. Bottom line is that fixing these safety and availability weaknesses provides direct benefit to the security of the code.
- See presentation slides at GitHub for more information. The FORTIFY spreadsheet is integrated into the slides. The spreadsheet will also be forwarded to the group.
- John is part of an effort with the National Society of Professional Engineers to resurrect the credentials on software engineering, to give it the same status as other engineering disciplines.
- NOTE: Many quality issues within previous MITRE Common Quality Enumeration (CQE) were later integrated into CWE for the reasons outlined.

Open Discussion

- The next CWE release is expected in the next couple days. It will include one new entry, and new observed and demonstrated examples.
- Look out for a change in the date, or cancellation, of the December meeting.

Reminders and Adjourn

- Next meeting is November 29 at 12pm EST.
- Questions of thoughts? Contact CWE@mitre.org or CAPEC@mitre.org.