HW CWE SIG Meeting
Friday, July 14, 2023

Members in Attendance

Gananand G Kini	Amitabh Das	Rich Piazza
Bob Heinemann	Thomas Ford	Shivam Swami
Gage Hackford	Joerg Bormann	Sohrab Aftabjahani
Donald Davidson	Steve Christey Coley	Farbod Foomany
Alec Summers	Abraham Fernandez Rubio	Carlos Moreno
Faheem Ahmed	Luke W Malinowski	Sayee Santhosh Ramesh
Alric Althoff	Jason Fung	Paul Wortman
John Hallman	Evan Bryers	James Pangburn
Scott Constable	Bruce Monroe	

Agenda

- Housekeeping and Announcements
- CWE Nit Bits (Bob Heinemann)
- CWE 4.12 Release Summary and new demonstrable examples (Bob Heinemann)
- Becoming a CNA (Alec Summers)
- Status of HW CWE Submissions (Steve Christey Coley)
- Most Important Hardware Weaknesses Refresh (Bob Heinemann)

Housekeeping

- Next meeting: Rescheduled from August 11 to August 18, 12:30 – 1:30 PM EDT (16:30 – 17:30 UTC) on MS Teams. Will send out an updated calendar invite.
- Contact: cwe@mitre.org
- Mailing list: hw-cwe-special-interest-group-sig-list@mitre.org
- Minutes from previous meetings: https://github.com/CWE-CAPEC/hw-cwe-sig

Announcements

- Top 25 update was released June 29.
- CWE 4.12 was released June 29.
- Tentative: CISA strategy around Secure by Design/Secure by Default for the August meeting.

CWE Nit Bits (Bob Heinemann)

- An experiment CWE is conducting to provide a recurring educational segment about CWE. Want to help the communities use CWE more effectively.
- Motivation came from experiences where we've provided educational material through IEEE HOST and some presentations to the SIG that received favorable feedback.
- Want the educational segments to be short, interesting, and recurring. We'll do a few and hopefully hear feedback from the community, to help determine whether to continue.
- Recently, a common terms Cheat Sheet was created. It's a subset of the glossary and includes terms thought to be most important and terms most likely to be encountered by users, e.g., Pillars, Classes, Bases, and Variant Weakness. Also includes common terms found in weakness titles, such as Resource, Information Exposure, Improper, Authentication and Authorization.

CWE 4.12 Release Summary and new DEMOXs (Bob Heinemann)

- Top 25 list was a major focus of 4.12 during the mapping process. There were few mappings to specific HW weaknesses (about 10 out of over 7,000). Will look through those to see if any can be used as observed examples (OBEXs).
- Version 4.12 also includes three new HW demonstrative examples (DEMOXs). These came from input derived from Hack@DAC 2019, the Technical University of Darmstadt, Texas A&M University, Intel, and the HW CWE SIG. New DEMOXs include GitHub links to see snippet code in full context where we can see the vulnerable code/bad code. The three new DEMOXs are:
    - CWE-1260: Improper Handling of Overlap Between Protected Memory Ranges
    - CWE-1262: Improper Access Control for Register Interface
    - CWE-1281: Sequence of Processor Instructions Leads to Unexpected Behavior
    - See slides for example vulnerable code and example fixed code for each new DEMOX.
- The three DEMOXs were selected from a batch of 38, and we're looking forward to receiving additional ones for HW. It would be great for HW SIG members to review them for correctness and suggestions to clarify text if needed.

Becoming a CNA (Alec Summers)

- CWE is a sister program with CVE where CVE Numbering Authorities (CNAs) are active. Organizations represented on this call may already be part of the CNA community.
- Trying to encourage a "de-siloing" between the two programs, specifically with the expansion into hardware in CWE over the last couple years. Want better mapping of HW CWEs (root cause) to CVE vulnerabilities.
- CNAs are organizations or individuals from around the world authorized by the CVE program to assign and publish CVEs within their scope. CNAs include vendors, researchers, open source, CERTs, hosted services, bug bounty providers, and consortiums.

- Over the past 7 years, there has been an emphasis on federation across CVE to encourage ownership of CVEs by organizations other than MITRE. In 2016, the program had only 24 CNAs and MITRE owned the large majority of CVE records. Today, there are 304 CNAs, and this represents a wider ownership of CVEs. MITRE ownership share of CVEs has gone down significantly as a result of federation.
- Benefits of becoming a CNA include demonstrating to customers and the community that you know vulnerability management practices and have a commitment to cybersecurity, and having control over the CVE publication release process for vulnerabilities within your scope, including owning the language/text of the vulnerability.
- No monetary cost to be a CNA, and no contract to sign, but time/human resources are needed to be effective.
- Requirements to become a CNA:
    - Have a public vulnerability disclosure policy (e.g., Microsoft). Additional examples of vulnerability disclosure policies can be found here.
    - Have a public advisory location (e.g., Apple).
    - Agree to the CVE Program Terms of Use.
- Process to become a CNA (see slides for full details):
    - Request information on how to become a CNA using the CVE Program webform here.
    - A member of the CVE Program Coordination Team will provide a link to the registration form and supplemental material.
    - Once the registration form is received, a one-hour onboarding session will be scheduled (with the selected Root or Top Level Root, based on CNA scope).
    - After onboarding session, you will be asked to complete and submit homework.
    - Once homework is submitted and approved, the CVE Program will work with you to select a date for announcement into the program.
    - After announcement, the CNA requests credentials to access CVE Services, and can then start requesting CVE IDs and publishing/updating CVE records in their scope.
- CVE Program expectations of CNAs:
    - Follow the CNA Rules and the CVE Program Professional Code of Conduct.
    - Adhere to the CVE Program policies, e.g., Record Dispute Policy, and EOL Policy (end of life).
    - Publish CVE Records in a timely manner once disclosure is made public
    - Once a vulnerability (and associated CVE ID) is made public (via an advisory, Tweet, blog, etc.), CVE Records must be published to the CVE List within 5 business days.
    - Respond to requests from your Root (or Top-Level Root) in a timely manner.

    - Communicate any changes to your CNA organization (POCs, mergers, change in scope) to your Root or Top-Level Root.
- Overview of the CVE Program organization chart presented (see slides). Not yet shown in the org chart are authorized data publishers (work in progress).

Status of HW CWE Submissions (Steve Christey Coley)

- CWE has 100+ HW related records. Most were made before the new external submission server and formalized review process were put in place in mid 2022.
- There are currently 13 submissions that are active and being processed (see slides for details):
    - 2 submissions: "Complex Domain / Classification"
    - 4 submissions: "Overlap / Subtree Overhaul (Access Control)"
    - 1 submission: "Overlap / Subtree Overhaul (Cryptography)"
    - 4 submissions: "Affected by Scope Exclusions"
    - 2 submissions: "Needs integration into existing content"
- Trying to improve the quality of HW submissions, and make the process easier to get to publication and inclusion in CWE.

Most Important Hardware Weaknesses Refresh (Bob Heinemann)

- A list of the most important hardware weaknesses was developed and released with CWE 4.6 in October 2021. It was put together using an empirical process and voting system. Current list is available here.
- Is this something the HW SIG should revisit and update? Have there been substantial developments since the last release that merit an update (there are four new HW entries to consider – see slides)?
- The HW SIG was asked to give this some thought.