HW CWE SIG Board Meeting #5

Friday March 19 @ 1230-1330 EST

Members in Attendance

Sohrab Aftabjahani – Intel
James Bellay - Batelle
Evan Bryers - Aerospace
John Butterworth – MITRE CWE
Steve Carlson - Cadence
Matthew Coles – Dell
Erik Costlow – Compass Security
Kerry Crouse – MITRE CWE
Steve Christey – MITRE CVE
Ashish Darbari - Axiomise
Amitabh Das - AMD
Nusrat Dipu - University of Florida
Thomas Ford - Dell
Farbod Foomany – Security Compass
Jason Fung – Intel
Kathy Herring Hayashi – Qualcomm
Marisa Harriston – MITRE (HW CWE SIG Secretariat)
Milind Kulkarni - NVIDIA
Vikas Kumar – Intel
Mohan Lal – NVIDIA
Chris Lathrop – MITRE CWE
Lang Lin – Ansys
Luke Malinowski - MITRE CWE
Parbati Manna - Intel
Bruce Monroe – Intel
Kirrill Motil - Microsoft
Jason Oberg – Tortuga Logic
Abhijit Parmar - Microsoft
Rohini Naraispur - Bosch
Muhammad Usama Sardar - Dresden University of Technology
Andreas Schweiger - Airbus
Robert Van Spyk – NVIDIA
Alec Summers – MITRE (HW CWE SIG Moderator)
Brent Sherman – Intel
Charles Timko - Analog
Jim Wesselkamper – XiLinx
Paul Wortman – Wells Fargo

Housekeeping

- The Github site is now public for access to the minutes
- Next meeting is April 16; 12:30 – 1:30 PM EST

CWE v4.4 and schema update

Refer to slides for additional details

- Updates were made to move schema to version 6.4
- On the hardware side, FunctionalAreaEnumeration (functional areas the relate to each applicable CWE) types were added; users will see the new "Functional Areas" field
- *Purpose:* Useful for search and quickly grouping related CWE's together (view filtering)
- Only items under 'Power' & 'Clock' were added; Next release will include items from remaining categories
- A **Deprecation Work Group** was created to get the communication involved in addressing overlap/duplication issues
    - Initially, the group will determine why CWEs may be overlapping versus whether or not they are duplicates of each other or if a parent/child configuration may need to be set up
    - Original submitters may be contacted to hear about which core weakness was being described and to collect other pertinent details
    - HW SIG will then be approached for buy-in on proposed changes
    - *Important note:* Once a CWE is submitted, it can't go through significant changes in scope to avoid confusing users. If a CWE is no longer useful, it may be deprecated and a new one could be developed. The CWE team follows established processes for prioritizing IDs to keep
    - Submitter credit will be preserved regardless of content status (exact process TBD)

Community Perspective: Submitting HW CWE content

Paul Wortman – Cyber Security Research Scientist, Wells Fargo

The presenter provided perspectives on the submission form which he described as straightforward:

- The hardest part of filling out the form was ensuring language was clear and concise enough to get points across
- CWE team has been diligent about following up on submissions that require clarification or to draw distinctions between other content
- Compiling the submission took about 30 to 40 minutes
- Working with the CWEs has helped education efforts and to develop a standard for the community to use from a hardware perspective.

A CWE team member asked if there was anything that could have been developed to help educate the speaker as a CWE user.

The speaker responded by saying that any confusion that occurred came from exploring weaknesses from having to learn industry language and coming from an academic background.

The moderator then addressed a question regarding the submission format, describing the text file that matches categories found on the individual CWEs. He also pointed members in the direction of guidelines, which are available on the CWE website. A streamlined web form is currently being created.

A member asked if submitters should be responsible for determining whether their content could be a duplicate. The moderator replied that they are not and directed anyone with questions before or while submitting to email the CWE team before investing the time in filling out a form.

A CWE team member mentioned that creating guidance would be a focus for the next 6 months/year. The current use case is on reporting publicly available vulnerabilities and how to find appropriate CWE identifiers.

A conversation about licensing submissions and some of the challenges of submitting content due to funding was brought by a member. Another member shared the process of working closely with their organization's legal team to ensure proprietary information is not included as well as a third-party consortium. The moderator reminded members to refer to the Terms of Use if there are questions or concerns and that CWE/CAPAC/CVE are all services facilitating the exchange of public knowledge.

2021? HW CWE Top *n*

Refer to slides for additional details

The moderator led a discussion on what a "Top" list (similar to the Top 25) focused on hardware could look like.

Survey Questions

- What types of questions would be valuable for SME participant orgs?
- What are your internal findings?

Other opportunities for data?

- Recent hardware-related CVEs (may require re-mapping effort)
- How far do/can we go back?
- External research, is this collected (and available) anywhere else?
- Could we use internally discovered weaknesses that were removed before the product was released?

Other Thoughts:

- How big should the list be?
- Strictly HW weaknesses?
- Do you have data on bugs, independent of security consequences? Or results from code analysis tools?

Members generally agreed that a survey would help with obtaining the necessary information.
A member suggested having members reference their own vulnerability lists (whether published or not) as well as tangentially related data as an alternative to working off of existing CVEs with the caveat that attributes would be scrubbed and proper approvals provided. Another member asked if the CWE team had worked with NIST/NVD to capture relevant CWE information from their submission process. The moderator confirmed that the teams work closely together on mapping and other efforts (e.g. view 1003). A CWE team member added that NIST/NVD recently created a tool (CV Map) that would allow

vendors of affected CVEs to submit custom data which could be another avenue for collecting information. A third member suggested developing a hardware equivalent of view 1003.

A member discussed the limitations for the severity categorization (one of the factors for the Top 25 list) for hardware. A CWE team member proposed the inclusion of "difficulty of the fix" as another factor. Another member suggested differentiating between whether there is a fix or a workaround. The moderator brought up the idea of making the list unranked.

At the end of the meeting, the moderator requested that members interested in helping to develop the survey reach out.