HW CWE SIG Board Meeting #4

Friday February 19 @ 1230-1330 EST

Members in Attendance

Sohrab Aftabjahani – Intel
James Bellay - Batelle
Mike Borza - Synopsys
John Butterworth – MITRE CWE
Dave Clinton - Microchip
Matthew Coles – Dell
Kerry Crouse – MITRE CWE
Steve Christey – MITRE CVE
Amitabh Das - AMD
Nusrat Dipu - University of Florida
Fidelia Floyd - Leidos
Jason Fung – Intel
John Hallman – OneSpin Solutions
Marisa Harriston – MITRE (HW CWE SIG Secretariat)
Victor Ibe – Aerospace
Milind Kulkarni - NVIDIA
Vikas Kumar – Intel
Mohan Lal – NVIDIA
Lang Lin – Ansys
Parbati Manna - Intel
Bruce Monroe – Intel
Kirrill Motil - Microsoft
Srinivas Naik – Intel
Jason Oberg – Tortuga Logic
James Pangburn - Cadence Design Systems
Sayee Santhosh Ramesh – Intel
Robert Van Spyk – NVIDIA
Alec Summers – MITRE (HW CWE SIG Moderator)
Brent Sherman - Intel
Jim Wesselkamper – XiLinx
Paul Wortman – Wells Fargo
Altaz Valani -Security Compass

Housekeeping: GitHub Access /Submission Transition

The moderator asked group members if they were comfortable with making the GitHub repository (containing meeting minutes) public versus invite only for ease of access. No one expressed concerns. He also shared that the content submission process may be transitioning to GitHub in the future.

A member expressed an interest in using GitHub for submissions because it would increase transparency and credibility toward the process.

The moderator shared that there is a new form coming for release 4.4 to help start the transition.

ACTION: Sending message to confirm that all group members are comfortable with switch to public access

Other housekeeping items:

- Next meeting is on 3/19 at 12:30 pm EST
- Point other potential participants to cwe@mitre.org

Developing Top 25 List for Hardware

See slides for more information

The moderator provided background on the changes in methodology overtime and CVE data usage for the CWE Top 25 Most Dangerous Software Weakness List. He then asked a series of questions to gauge were there was interest from the group in creating an analogous top list for hardware design weaknesses.

A member shared that a subgroup is currently working with CVE to implement tagging that is hardware and software specific as an example of an approach that could make compiling a top list easier. There has been some pushback. The moderator asked if pushback was as a result of CNAs having to go back and make updates. The member shared that there would be an optional field moving forward while acknowledging that backtagging might be a challenge.

A CVE team member asked if there has been more anchoring based off of CPE (Common Platform Enumeration; common identifier for a product). After a discussion around the topic it was determined that more information would be needed regarding the level of details currently available before inclusion is considered.

Several members discussed the possibility of surveying the industry to get a less formal top list as a short term solution/starting point. The moderator then asked about how the criteria for the most critical software weaknesses can be determined.

A member shared that one thing to consider is criteria around impact because for example, some vulnerabilities might not be able to be patched so the group might want to expand on the definition of severity to make the list more effective. He recommended limiting the number of vendors focused strictly on hardware to get the right level of information.

Another member recommended bringing a diverse mix of organizations beyond hardware focused organizations (e.g. chip vendors) together to get the right lens when development begins.

There was a discussion between a CVE team member and a member about how and why NVD doesn't have hardware mapped. An informal poll was also taken to determine how many members are currently using/engaging with/testing use of the hardware CWEs. Approximately 12 group members shared that they were on some level.

A member suggested focusing education efforts for the potential new list so that they coincide with Cybersecurity Awareness Month. A conversation then took place around the challenges of distinguishing the lines between weaknesses in hardware, software, and firmware and the importance of capturing chaining between weaknesses and vulnerabilities.

Another member asked about what the group can do to assist with education efforts. A canned presentation came up as an idea. The moderator suggested developing a condensed 101 deck for members to share with special interest groups.

ACTION: Develop and eventually post slides for the group's use to use on GitHub.

CWE Minor Release, Version 2.2

See slides for more information

- Release Date: March 15
- Using this period of lower growth (fewer submissions) to perform maintenance and QA on current entries

The group briefly discussed the recognition of submitters and changes that would be occurring.

Future Volunteer Presenters

- Leveraging HW CWE in your organization and/or operations?