HW CWE SIG Meeting
Friday, January 13, 2023

Members in Attendance
Bob Heinemann - MITRE
Jason Fung
Priya Iyer
Nicole Fern
Arun Kanuparthi
Luke W Malinowski – MITRE
Gananand G Kini
Parbati K Manna
Allen Krell (Guest)
Milind Kulkarni (PSIRT) - Nvidia
Steven M Christey - MITRE
Ford, Thomas - Dell
Wortman, Paul – Wells Fargo
Khattri, Hareesh - Intel
Michael Pak (Guest)
Alec J Summers - MITRE
Kumar, Vikas - Intel
Connor Mullaly – MITRE
Scott Constable – Intel
Mohan Lal - Nvidia
Coles, Matthew - Dell
Rich Piazza - MITRE
Jason Oberg (Guest)
Sanaka, Naveen - Dell
Jim Barry Jr. - MITRE
Ramesh, Sayee Santhosh - Intel
DiMase, Daniel - Aerocyonics Inc
Walters, Steven - Aerocyonics Inc
Sebastian Fischmeister - University of Waterloo
Evan Bryers
James Pangburn - Cadence
Lang Lin - Ansys
Wesselkamper, Jim - AMD
Farbod Foomany - SecurityCompass
Andreas Schweiger - Gast
Carlos Moreno – Palitronica

Agenda
- Housekeeping
- Announcements
- Working Items for this Meeting
    - Scope exclusions (updates and changes): Will be made public on the website after this meeting.
    - Transient Execution Weaknesses Update: Progress report and call for participants.
    - CWE-319 rephrase to include HW: Content of CWE-1324 as a JTAG Demonstrative example.

Housekeeping
- Next meeting: February 10, 2023, 12:30 – 1:30 PM EST
- Contact: cwe@mitre.org
- Mailing list: hw-cwe-special-interest-group-sig-list@mitre.org
    - All mailing list items are archived publicly at: https://www.mail-archive.com/hw-cwe-special-interest-group-sig-list@mitre.org/
- Minutes from previous meetings: https://github.com/CWE-CAPEC/hw-cwe-sig

Announcements
- CAPEC targeted for January 24, 2023
- CWE 4.10 targeted for January 31, 2023

- New ICS/OT SIG Working Groups launched. “Boosting CWE Content” group is impacting HW CWE (updates and additions to HW CWE).
- Mailing List Discussion: CWE Mappings to potential categories: “Hardware Trojans,” “Reverse Engineers,” and “Untrusted Manufacturing.”

Scope Exclusions Updates and Changes (Steve Christey)

- So far, there are 10 scope exclusions that were developed during 2022.
- Started integrating scope exclusions into review process for submissions summer 2022.
- There have been few hardware submissions to date.
- Scope exclusion issues may also apply to existing CWEs.
- Exclusions will be published to cwe.mitre.org soon, and are not yet official. Community comment and discussion is important before approval. Formal approval process is TBD.
- There was a presentation about exclusions of interest to the HW SIG:
    - SCOPE.HUMANPROC - Human/organizational process
    - SCOPE.NOMITS - No actionable mitigations
    - SCOPE.CUSTREL - Not customer-relevant
    - SCOPE.CONFLICT - Conflict/contradiction with other weaknesses
- If the program decides to accept weaknesses with no actionable mitigations, they could be used for new research and added to the existing ‘research gaps.’

Transient Execution Weaknesses Update (Gananand Kini)

- Working on trying to define weaknesses related to transient execution.
- Trying to get to a state where they can be processed as a CWE entry.
- Need better descriptions of the weakness and the conditions that lead to the weakness.
- Descriptions and extended descriptions are in-work; feedback welcome using the Box platform.
- Four proposed CWE submissions:
    - SUB-CWE-B: Transient Data Forwarding from an Operation that Triggers a Processor Event
    - SUB-CWE-C: Transient Execution Influenced by Shared Microarchitectural Predictor State
    - SUB-CWE-D: Microarchitectural Predictor causes Transient Execution
    - SUB-CWE-A: Processor Event Causes Transient Execution (catch all for transient execution issues that do not fall under the previous CWEs).
- If a microarchitectural feature is found to be exploitable and requires a CVE, then a reference to a CWE is required (cannot reference a category).
- To participate, contact cwe@mitre.org, attend the discussion group, or discuss on the HW CWE Mailing List.

CWE-319 Rephrase to include HW: Content of CWE-1324 as a JTAG Demonstrative Example

- CWE 4.10 will include an update to CWE-319: Cleartext Transmission of Sensitive Information. Its scope has been expanded to include hardware weaknesses.

- CWE-319 has some overlap with CWE-1324: Sensitive Information Accessible by Physical Probing of JTAG Interface…
- The proposal was made to rely on the updated CWE-319 scope to address the weakness of transmitting cleartext for both hardware and software. Then CWE-1324 would be deprecated as a CWE, but used as an example case under CWE-319. Will help centralize concerns about unencrypted communications and improve usability for the underlying weakness.
- Other changes in 4.10 include: global replacement of the term “software” with “product.”