HW CWE SIG Meeting

Friday, October 14, 2022

Members in Attendance

Aftabjajani, Sohrab	Heinemann, Bob	Mullaly, Connor
Coley, Steven	Kini, Gananand	Naveen, Sanaka,
Constable, Scott D	Kumar, Vikas	Oberg, Jason
Das, Amitabh	Labbato, Mark	Pak, Michael
Davidson, Donald	Lal, Mohan	Pangburn, James
DiMase, Daniel	Lathrop, Chris	Piazza, Rich
Dipu, Nusrat Farzana	Lin, Lang	Roberge, Robert
Fern, Nicole	Malinowski, Luke	Summers, Alec
Ford, Thomas	Manna, Parbati K	Taggart, Phillip
Fung, Jason M	Matthew, Coles,	Timko, Charles
Hackford, Gage	Monroe, Bruce	Wortman, Paul

Introduction, Announcements, and Agenda

MITRE CWE: Steve Christey Coley

- Topics: Microarchitectural weakness and changing execution.
- Reschedule of November meeting to November 11 due to Veteran's Day, calendar update sent
- December meeting also pushed back a week; calendar update sent.
- CAPEC v3.8 released on September 29, 2022.
- CWE v4.9 released on October 13, 2022.
- New ICS/OT SIG Working Groups launched. "Boosting CWE Content" group to examine gaps in CWE.
- Scope Exclusions and Submission Problems are to be posted for public review in late October.

Hardware Items in 4.9 Release

MITRE CWE: Steve Christey Coley

- See the slide deck for a complete summary.
- Changes about names, categories, new CWE related to weak credentials.

Call for Next Release Priorities

MITRE CWE: Bob Heinemann

- Call the community for involvement.
- If there are priorities from community members, please provide your input.
- Reviewed Working Queue items.
    - Community tagged or labeled (been submitted by a community member)
    - Internally generated items

Transient Execution Weaknesses Update

MITRE CWE: Gananand Kini

Commented [SMC1]: Gananand

- Notes from September 21 Meeting.
- Discussed potential "partitions" for defining weaknesses in transient execution with Scott Constable and Nicole Fern as part of a meeting on September 21.
- Spurred by the HCWE109 submission, we decided to try to identify the root causes rather than looking at existing CWEs.
- Instead focused more on how transient execution feature implementations could allow for certain dangerous behaviors.
- We continue working with Scott Constable, Nicole Fern, and Jason Oberg to refine transient execution weaknesses in CWE.
- Don't have to define weaknesses per vulnerability but look at root causes as to why the vulnerability exists.
- Can chain weaknesses together. The idea is a weakness can be chained to another, which eventually leads to a vulnerability.

Improving CWE Coverage for Weaknesses that Relate to Transient Execution

Intel: Scott Constable

Commented [SMC2]: Why copy these slides? They're in the original presentation, right?

- Review of current transient execution related CWEs.
- CVE vulnerabilities related to transient behavior of SMC (Self Modifying Code) may not fit with the existing CWE A, CWE B and CWE C proposed and hence deserves a new CWE D (on slide 15).
- Discussion will continue with a small group of MITRE and SIG members. If interested in participating, please email cwe@mitre.org.

Closing Questions

- A member asked how 1303 would fit into the transient weakness discussion and the new proposed categories.
    - **Response:** It could already fall under a CWE related to insufficient technical documentation. The talk on transient weakness was about stepping back and what that would look like if we started from scratch.
- A member asked what will be shown for CWEs and how this will impact the different views and personas. Is there anything of note we need to reflect in that effort to address any of the hardware CWEs?
    - **Response:** Most of the current discussions have been at a very high level and independent of the actual content of the CWEs.
    - Idea is to let the community play with the different views and then give recommendations.
    - Discussion concluded that both programs needed to ensure they were connecting the dots between efforts.