CVE Board Meeting Notes

October 26, 2022 (9:00 am – 11:00 am EDT)

Agenda

- 9:00-9:05 Introduction
- 9:05-10:25 Topics
  - WG Updates
  - Welcome New Board Member
- 10:25-10:35 Open Discussion
- 10:35-10:55 Review of Action Items
- 10:55-11:00 Closing Remarks

New Action Items from Today's Meeting

Action Item #	New Action Item	Responsible Party	Due
10.26.01	**Identify HW vendors participating in CVE Program; compare CWE HW SIG membership to CNA membership and report results.**		
10.26.02	**Develop new board member welcome kit.**	**Secretariat**	

Working Group Updates

- Automation Working Group (AWG)
  - During October, the AWG focused on CVE Services 2.1 soft deployment.
  - The two phases of soft deploy went as planned and ended October 25.
  - A few issues (from a down-convert perspective) between JSON 4 and JSON 5 were identified during soft deployment. None were show-stoppers, and hard deployment will proceed as planned. Messaging to the user community about these issues will be discussed at the TWG meeting on October 27.
- Outreach and Communications Working Group (OCWG)
  - Working with CNACWG; blog content has been developed and posted.
  - Current project is developing messaging to help counter concerns or objections to becoming a CNA.
  - Next project will be making sure that 2023 Summit content can be recorded, and that content can be broken out into discrete topics for viewing/reuse.
  - OCWG meeting attendance has been up and down lately, and some key members have moved on.
- CNA Coordination Working Group (CNACWG)
  - There have been some new CNAs participating in the WG meeting.
  - CNAs have expressed interest in the upcoming workshop, so they can learn more about the new CVE services.
  - The chair suggested that maybe the CNA Operational Rules could be updated more frequently/incrementally (continuous integration, continuous deployment –

CICD), rather than just a 'big' version update that occurs less frequently. There is a sense the CNA community would like that and benefit.
    - The idea would be to update continuously for small or quick updates, but still have significant version updates as needed for bigger and more time-consuming changes.
    - Incremental updates would be reserved for those that do not disrupt a CNA's workflow.
    - The change would require 'retooling' of the current update process and selection of the technology or platform to use. It would also require criteria/rules to distinguish a small update from a big update.
    - Members liked the idea, and there was agreement by the Board members in attendance to ask the SPWG to flesh out the idea for further consideration.
- Quality Working Group (QWG)
    - Version 5 schema has been finalized and released.
    - About 15 issues have been identified with the new schema and these will be addressed in version 5.1. One example is users would like the ability to add hardware version identification to a CVE Record.
    - None of these issues are major or interfering with CNA work.
    - It was suggested to leave 5.0 in place long enough to identify other issues that may have not been discovered yet, given the early stage of deployment.
    - QWG will collaborate with AWG to define the 5.1 updates and determine a logical time to release.
    - Slides/content about potential schema updates and timing will be prepared by QWG for the upcoming CVE Services 2.1 workshop on November 2.
- Transition Working Group (TWG)
    - Recent activity has focused on preparing for the workshop on November 2.
    - A member asked about current status of the next bulletin to the user community.
        - AWG and OCWG worked together to draft Bulletin #11. The next step is review by TWG, hopefully at the TWG meeting on October 27.
        - Target posting/publishing is by the end of this week.
- Strategic Planning Working Group (SPWG)
    - The current major activity is finalizing the CVE Program Governance and Organization document. No set timeline yet for completion.
    - The next big activity will be finalizing the CNA Operational Rules update.

Welcome New Board Member

- Pete Allor (Red Hat, Inc.) is the Board's newest member, as of October 24.

Open Discussion

- CVE Record Dispute Policy
    - A researcher filed a dispute for CVE record 2022-28958, which is on the CISA KEV list. The researcher disputes that the vulnerability is a real vulnerability.
    - The dispute was filed October 3 (est.), and after three weeks, the researcher had not heard back about status of the dispute.
    - The recent Dispute Policy update specifies SLAs that have already been missed.
    - The Secretariat will look into what happened with this dispute, and how there can be better communications about dispute process status.
    - Disputes about records on the KEV list should be communicated to CISA.
- Hardware CVE Records

    - NIST has responsibility under the CHIPS Act which is about improving chip capability production capabilities in the U.S. and improving security in hardware.
    - There have been recent discussions between NIST and stakeholders about this subject, and some feedback has been provided about the lack of CVE records for hardware vulnerabilities.
    - It is not always easy to identify a hardware vulnerability. Some vulnerabilities are easy to distinguish between software or hardware, but in other cases it is not clear. Better definition of a hardware vulnerability would help.
    - It is not currently easy to query records to identify which ones (or how many) are hardware vulnerabilities. How can the program get better data for this? Also, how can the program improve its process for assigning hardware vulnerabilities?
        - NIST is interested in getting experts together to look into how to answer these questions. Are members of the Board interested? An email will be sent to the Board to gauge interest.
        - Maybe add a hardware tag to the record.
    - The question was asked about the level of hardware vendor CNA involvement in the CVE Program. The program will look into this and report back. A review of which CWE HW SIG members are CVE CNAs will be conducted and the results reported to the Board on the private email list.
    - Members of the program will attend a CWE HW SIG meeting to discuss the value proposition of participating in CVE.
    - The suggestion was made to provide guidance on how to choose the correct communication channel for different messaging/audiences. For example, private or public list, Slack, Discord, etc. The Secretariat will include this information in a new board member welcome kit. A Board channel in Slack was created during this discussion, and the link will be provided via email.
- JSON 5.0 Character Limits
    - The Secretariat sent an email to NIST concerning whether JSON 5.0 character limits affect NVD's ability to pull data from CVE.
    - Questions about/for NVD can be directed straight to them.

Next CVE Board Meetings

- Wednesday, November 9, 2022, 2:00pm – 4:00pm (EST)
- Wednesday, November 23, 2022, 9:00am – 11:00am (EST)
- Wednesday, December 7, 2022, 2:00pm – 4:00pm (EST)
- Wednesday, December 21, 2022, 9:00am – 11:00am (EST)
- Wednesday, January 4, 2023, 2:00pm – 4:00pm (EST)
- Wednesday, January 18, 2023, 9:00am – 11:00am (EST)

Discussion Topics for Future Meetings

- CVE Services 2.1 updates (on-going)
- Working Group updates (every other meeting)
- Council of Roots meeting highlights (aligned with Council of Roots meeting dates)
- Researcher Working Group proposal for Board review
- Vision Paper and Annual Report
- Secretariat review of all CNA scope statements
- Proposed vote to allow CNAs to assign for insecure default configurations