CVE Board Meeting Notes

November 9, 2022 (2:00 pm – 4:00 pm EST)

Agenda

- 2:00-2:05 Introduction
- 2:05-3:25 Topics
  - CVE Services Workshop Post Discussion and Survey Results
  - Identify Hardware Vendors Participating in the CVE Program (compare CWE HW SIG membership to CNA membership and report results)
- 3:25-3:35 Open Discussion
- 3:35-3:55 Review of Action Items
- 3:55-4:00 Closing Remarks

New Action Items from Today's Meeting

Action Item #	New Action Item	Responsible Party	Due
11.09.01	**Under CNA Type, create a new Open-Source Project option (separate the current option: Vendors and Projects).**	**Secretariat**	
11.09.02	**Set up a meeting to discuss prioritization of CVE Services issues, with respect to References.**	**AWG**	
11.09.03	**Develop scenario examples related to CVE vulnerabilities.**	**Board Member**	**11/30/22**

CVE Services Workshop Post Discussion and Survey Results

- A survey was sent to workshop participants. Response rate was low (13 out of all participants), but that feedback was positive, except for one participant who indicated a question(s) was not addressed. One participant commented to have more live demos.
- Many questions were answered during the workshop in chat and the back channel.
- The AWG will review the current FAQs to determine what should be added.
- The workshop chat will be reviewed to identify user information needs that could be addressed in a Bulletin, FAQ, or other method.

Identify Hardware Vendors Participating in the CVE Program

- This action item (10.26.01) purpose was to identify hardware vendors participating in the CVE Program and compare them with hardware vendors participating in the CWE Hardware SIG Group. The action has been completed, and results can be used to identify HW vendor candidates for CNA recruitment.

Open Discussion

- Distinction between Vendor CNA and Open-Source Project CNA

    - It was recommended that the program make a distinction between a vendor CNA and an open-source project CNA. Currently, CNA Type combines vendors and projects in a single category. If a CNA is not both, then they should not be listed as both. There were no objections to looking into this further (action item).
    - It was mentioned that a CNA may fall under both Types, which is fine.
    - Some CNAs may fit in multiple categories, but this discussion is about making sure open-source project CNAs are easily identifiable.
- Swagger
    - A vulnerability was identified in Swagger (the 'Try Me' feature caches the user's API key in the browser). It should be identified/recorded as a CVE and Swagger should be notified.
- CVE Services 2.1 Next Steps
    - The development team is working on issues identified during Soft Deployment that need to be fixed prior to Hard Deployment. There are 36 issues (many related to down convert capability) and they are organized into high or low priority.
    - High priority issues are listed on the GitHub.io site, and as fixes are implemented, the user community will be notified.
        - Automating reference capabilities is one of the items on the high priority list.
    - There is significant interest from the user community about when the ADP pilot will start. There are questions about ADP policy and rules that need to be addressed.
        - More work is needed to define requirements and use case scenarios before a time estimate can be made.
        - Current development team focus is on the high priority issues identified during Soft Deployment.
        - There will be an off-line or out-of-cycle meeting to discuss whether ADP capability needs to be in place prior to Hard Deployment (i.e., add to hard deploy priority list).
- Multi-factor Authentication (MFA) to CVE Services
    - Requirements for MFA have not been defined. With program growth, this will become more important, so it needs to be on the roadmap of service updates. It is not currently on any near-term roadmap.
- New Working Group Idea
    - The idea was introduced to create a working group to develop a 'playbook' of interesting scenarios regarding CVE, especially with respect to cloud vulnerabilities. This may help clarify the distinction between a vulnerability and an issue that is not a vulnerability.
    - Initial scenario examples will be prepared for the next Board meeting (action item). This will help inform whether a new working group is needed, or if an existing working group can do it.

Review of Action Items

- 10.26.01 has been completed and results were shared at today's meeting.

Next CVE Board Meetings

- Wednesday, November 30, 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)

- Wednesday, February 1, 2023, 2:00pm – 4:00pm (EST)

Discussion Topics for Future Meetings

- CVE scenario examples (scheduled for November 23 meeting)
- CVE Services 2.1 deployment updates (on-going)
- Working Group updates (every other meeting – next scheduled for November 23)
- 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