CVE Board Meeting Notes

December 14, 2022 (2:00 pm – 4:00 pm EST)

Agenda

- 2:00-2:05 Introduction
- 2:05-3:25 Topics
  - CVE Program Summit Date
  - CNA Type Label Wording: Vendor, Open Source Project, Consortium
  - Adding .csv Format for Downloads
  - CVE Program and WG Priorities for First Half of 2023
  - Playbook: Examples of Interesting CVE Scenarios
- 3:25-3:35 Open Discussion
- 3:35-3:55 Review of Action Items
- 3:55-4:00 Closing Remarks

New Action Items from December 14 Meeting

Action Item #	New Action Item	Responsible Party	Due
12.14.01	**Develop definitions for the CNA Types for presentation to the Board, prior to making available to CNAs.**	**Secretariat**	
12.14.02	**Send request to all WG chairs (and other Board members) asking for input on 2023 priorities from their perspective.**	**Secretariat**	**12/16/22**

CVE Program Summit Date

- Discussion continued from the last Board meeting about the date and location of the Summit in early 2023.
- MITRE has reserved an auditorium for the event at its campus in McLean, VA, for March 22-23, 2023. The auditorium is outside of the security perimeter which will make access more convenient for visitors. There will also be an option for people to attend virtually.
- Proof of COVID vaccination is required for visitors to enter MITRE facilities. A picture of the vaccination card will suffice. This information will be included in future communications.

CNA Type Label Wording: Vendor, Open Source Project, Consortium

- The program has labels for different CNA types. The following changes were adopted:
  - "Vendors and Projects" becomes "Vendor" (singular)
  - "Open Source Project" becomes "Open Source"
  - Added "Consortium"
  - "Vulnerability Researchers" becomes "Researcher" (singular)
- Definitions will be developed for each of the CNA types and shared with the Board prior to making available to CNAs.

- CNAs will be asked to review their label/type, and the label selection decision is theirs. They may select more than one type as appropriate.

Adding .csv Format for Downloads

- Losing the capability to download CVE Record data in .csv format is problematic for many consumers of CVE data. The Board previously decided to make downloads available in JSON 5 format only. Should .csv format be continued?
- The current .csv format has 7 fields, only 4 of which are still used by the program.
- There was agreement to keep the .csv format download capability for a temporary period as users continue to adjust to JSON 5.
    - The current format will stay the same, with explanatory note(s) added about the fields that are no longer used, and to point users to JSON 5 format for more enriched data.
    - The note about the unused fields will be incorporated in a way that avoids breaking anything in the user download experience.
- A request for a JSON 5 to .csv format converter will be taken to the Automation Working Group (AWG), but there was Board agreement that other AWG priorities, e.g., user registry, ADP pilot should be addressed first. A converter will be available prior to discontinuing .csv download capability.

CVE Program and WG Priorities for the First Half of 2023

- A request to WG chairs and other Board members will be sent this week asking for input on program priorities for next year.
- Input is due in time to have a discussion at the next Board meeting on January 4, 2023. A reminder will be sent the last week of December.

Playbook: Examples of Interesting CVE Scenarios

- There was a meeting earlier on December 14 with two Board members and other external (to CVE) participants.
- The external participants expressed that they were not happy about the rules for cloud vulnerabilities. There have been concerns about what are good practices for dealing effectively with vulnerabilities in a cloud environment. They want more transparency around where the line is for a cloud provider to assign or not assign a CVE.
- The current rules are generic in how the program defines and addresses vulnerabilities, including for cloud vulnerabilities. More targeted rules or program guidance are needed to help the community identify a vulnerability in different environments, e.g., by using a decision tree.
- The Board was asked what they thought the role of the CNA of Last Resort is, in the context of assigning CVEs for cloud vulnerabilities. There was no disagreement to waiting for updated rules/guidelines for vulnerability assignment before answering this.

Open Discussion

Out of time.

Review of Action Items

Out of time.

Next CVE Board Meetings

- 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)
- Wednesday, February 15, 2023, 9:00am – 11:00am (EST)
- Wednesday, March 1, 2023, 2:00pm – 4:00pm (EST)
- Wednesday, March 15, 2023, 9:00am – 11:00am (EDT)

Discussion Topics for Future Meetings

- CVE Services 2.1 and program website updates (on-going)
- Working Group updates (every other meeting, next is January 4, 2023)
- Council of Roots meeting highlights (next is January 4, 2023)
- 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
- CVE Communications Strategy