CVE Board Meeting Notes

July 19, 2023 (2:00 pm – 4:00 pm EDT)

Agenda

- 2:00-2:05 Introduction
- 2:05-3:25 Topics
  - CISA ICS Top-Level Root Name, Scope, and Structure Change
  - AI/ML Vulnerabilities
- 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

New Action Item	Responsible Party
Check with CISA to get their feedback on: (1) making ICS a Root under CISA instead of a CNA, and (2) expanding scope (and changing name) of the proposed Federal Enterprises CNA to include state, local, territorial, and tribal governments. Update slides and distribute to the Board list for further comments and resolution.	**Board Member**
Invite NVIDIA to attend the Board meeting on August 16 to discuss AI/ML vulnerabilities. Inform Secretariat so it can be added to the agenda.	**Board Member**
Share AI/ML vulnerabilities bug bar with the Board when it is published.	**Board Member**

CISA ICS Top-Level Root Name, Scope, and Structure Change

- There have been recent discussions about expanding the CISA ICS Top-Level Root (TL-Root) scope to include Federal Enterprises. The MITRE TL-Root and the Secretariat support the intent and have provided feedback.
- Under the new structure, CISA ICS would drop ICS from its name, remain a TL-Root, and retain its CNA of Last Resort (CNA-LR) role. It would have two new CNAs under it: ICS and Medical Devices, and Federal Enterprises. Both CNAs could become Roots in the future, if needed.
- Question: Why not make ICS a Root under CISA immediately? Answer: Will check with CISA and get their thoughts (action item).
- Question: What kind of vulnerabilities are we expecting the Federal Enterprises CNA to focus on? Is it product related or open source related? Answer: One example is the numerous applications the federal government develops for citizens, e.g., booking time at a national park.
- Question: What are the expectations of the Federal Enterprises CNA? Would a federal agency become a CNA? Answer: No current expectations that a federal department or

agency will become a CNA, but if they want to become a CNA, it would make sense to elevate Federal Enterprises to the Root level.

- Comment: Do not limit Federal Enterprises scope to federal civilian agencies; include state, local, territorial, and tribal. Maybe call it Government (or .GOV) to allow more flexibility and expansion capability. Response: Will check with CISA and get their thoughts (action item combined with action item above).
- The slides will be updated, incorporating CISA's feedback. The updated slides will be distributed on the Board list for additional comments and resolution on this topic (action item combined with action items above).

Artificial Intelligence (AI)/Machine Learning (ML) Vulnerabilities

- Need an understanding of the scope of AI/ML vulnerabilities that fall within CVE purview, to help guide CNAs. For example, a model training issue is not a vulnerability.
- The program needs to send out public commentary to help the community understand its position on AI/ML vulnerabilities. What is and what is not a vulnerability in this space?
- There was a recent email exchange between a Board member and NVIDIA on this topic. Question: Would it be possible for NVIDIA to come talk to the Board about this topic and what their specific concern is? Answer: I think they would be receptive to the opportunity. An invitation will be extended to NVIDIA to attend the Board meeting on August 16 (action item).
- Comment: A Board member's company plans to publish a bug bar around the topic of AI and vulnerabilities in the near future. Could be a good data point for the program's guidance (action item).
- Comment: Would be useful to have a conversation with companies to understand their expectations around their security model in terms of AI/ML.
- Question: When we talk about making a statement to the community, do we mean a general statement, or something more codified? Answer: Treat it like we are treating cloud; do both.
- Question: Is this a topic we can resolve quickly enough to include in the next CNA Rules update (currently under revision)? Answer: No, the draft update is expected to be released in late August. Need more time to get AI/ML right.

Open Discussion

- JSON 4 Deprecation
    - Question: Did program guidance go out to the community about deprecating JSON 4 on June 30, 2024? That guidance was planned for the week after July 4. Answer: Yes, multiple messages have gone out about deprecation, but the specific June 30 date is awaiting TWG review. Decision could be as soon as tomorrow.
    - This is important, need to give community time to adjust.
- JSON 5 Guidance for CNAs/Developers
    - Question: What is the status of getting JSON 5 guidance out the door? Answer: Content is under development, and will need review by TWG and QWG before release. That should happen in about two weeks.
    - Intended to be a guide of top things to watch out for as a CNA/developer when interfacing with the updated CVE services.
- ADP References Pilot
    - Expect to push out to the ADP demonstration environment by end of next week.
    - Still expect to have the production pilot ready by end of August/early September.

    - Question: The CISA pilot may be done before the Secretariat (references) pilot. Does anyone see a reason why we should not just proceed with the CISA pilot first? Answer: They are independent; the order does not matter.
- ADP Application Template
    - CVE has been approached by several organizations that want to become ADPs. Need to bring some structure to the application process and establish requirements/criteria.
    - Previous action item – should be ready for SPWG review next week.
    - Application process will need Board review/approval.
- Executive Board session
    - A Board member requested an executive Board session to address private Board business. The meeting will be two hours and held August 2. As per the Board Charter, only official Board members can attend an executive session.
- Council of Roots and Working Group Updates
    - Slides will be submitted by WG chairs and presented/discussed during the August 2 Executive Board session.

Review of Action Items

None.

Next CVE Board Meetings

- Wednesday, August 2, 2023, 9:00am – 11:00am (EDT) – (Executive Session – Board only)
- Wednesday, August 16, 2023, 2:00pm – 4:00pm (EDT)
- Wednesday, August 30, 2023, 9:00am – 11:00am (EDT)
- Wednesday, September 13, 2:00pm – 4:00pm (EDT)
- Wednesday, September 27, 2023, 9:00am – 11:00am (EDT)
- Wednesday, October 11, 2023, 2:00pm – 4:00pm (EDT)

Discussion Topics for Future Meetings

- Review draft charter for new working group (for Summit planning, Annual Report, and the upcoming CVE 25th anniversary)
- Sneak peak/review of annual report template SPWG is working (June timeframe)
- Bulk download response from community about Reserved IDs
- Finalize 2023 CVE Program priorities
- CVE Services updates and website transition progress (as needed)
- Working Group updates (every other meeting)
- Council of Roots update (every other meeting)
- 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