CVE Board Meeting Notes

August 30, 2023 (9:00 am – 11:00 am EDT)

Agenda

- 9:00-9:05 Introduction
- 9:05-10:25 Topics
  - Working Group Updates
  - CVE (malicious) Link Rot Problem
  - AI/ML Vulnerabilities
- 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

New Action Item	Responsible Party
Schedule a meeting to discuss the non-responsive domain reference problem in CVE Records. Include CNACWG, QWG, and AWG.	**Secretariat**
Reach out to Google to ask if they would present on their research into AI-driven fuzzing to automate CVE assignments.	**Secretariat**

Working Group Updates

- Automation Working Group (AWG)
  - Provided technical guideline contributions to the Secretariat for the CVE Services guidance documentation.
  - Engaged with the QWG on how to effectively support use of JSON 5 by downstream users.
  - An ADP demonstration environment has been set up since June. CISA is using it and they have reported some initial results. The ADP references pilot is scheduled for delivery in late September.
- Outreach and Communications Working Group (OCWG)
  - Published a Q2 CVE Program Summary blog and working on an "Our CVE story" blog with F5 (target publish date of mid to late September).
  - In process with three podcasts: CVE JSON 5 records format; refresher of the popular Working Groups podcast (in the process of reaching out the chairs to schedule); another Roots podcast to reflect new Roots and their experiences.
  - Have completed the scripted slides for the updated CVE introductory video on YouTube, and have revitalized the format. Working to streamline video updates going forward. Will be presented to the TWG on August 31, followed by review by the Board using the private email list.

- CNA Community Working Group (CNACWG)
    - Have been working on the link rot effort (see next topic).
    - Reached out to the current mentors and proteges to remind them that they are in the CNA mentor program and suggest screen sharing (i.e., Mentors shoulder-surfing to guide mentees through their initial CVE Record processing).
- Quality Working Group (QWG)
    - Have cutover what is called a release candidate for schema micro release 5.01, and it is being tested. Going through some issues found. The 5.0.1 release should not affect anyone's processes or any existing CVE Records.
    - Working on a best practices guide for use of the schema for encoding things in a CVE Record.
    - Question: Does the QWG have anything in backlog right now that would be appropriate for a major release? Answer: Yes, we have a bunch of things for a major release, e.g., changing the schema to stop allowing blank spaces before and after text field entries. A change like that takes planning and coordinating with the CNA community to implement.
    - The Secretariat has prepared a related document draft CVE Services Guide that is being reviewed by the TWG.
- Strategic Planning Working Group (SPWG)
    - Initial draft of the updated CNA Rules document is expected late September for an internal program review. The CNAs will then be asked to review. The program will adjudicate CNA comments and provide a version for Board review.
    - After this update, will have a process to update the Rules more consistently, without having to do a major re-do.
- Tactical Working Group (TWG)
    - Launched a CVE Program 'Ideas and Suggestion' board August 29 on GitHub; coordinated with AWG and OCWG.
    - Also working on an article in Dark Reading that describes the changes the CVE Program has made over the years and inviting the community of users to take advantage of the changes. Hope to have out in next couple of weeks.
- Vulnerability Conference Working Group (VCWG)
    - The draft conference announcement is almost done. When final, the call for papers will be prepared and distributed.
    - Next step for the charter is working group approval.

CVE (malicious) Link Rot Problem

- Presentation shared titled "CVE Reference Investigations."
- CVE Record references have requirements, i.e., have to be good and accessible. This is not the case for many references.
- Recommendations to address this problem:
    - QWG: Take up this issue, as dead domains directly impact CVE data quality. Should have some way to check that references are good when a CVE Record is submitted.
    - AWG: Implement an on-the-spot archival procedure for references when CVEs are first submitted.
    - CNACWG: Encourage CNAs to archive their references.
    - Secretariat: Investigate the feasibility and impacts of hot swapping link destinations to archived sources.

- Secretariat will schedule a meeting to get into more detail about this problem. Include CNACWG, QWG and AWG chair or representative (action item).

AI/ML Vulnerabilities

- Guest speakers from NVIDIA and Microsoft shared their thoughts on AI/ML vulnerabilities
- Layers of an AI/ML-enabled application are application integration, framework, and ML model. Most ML attacks can be stopped at the application integration layer.
- In the ML model layer, vulnerability "poisoning" can occur during data collection/processing, training, or inference.
- Bad assumptions lead to flawed design, which can lead to vulnerabilities.
- Discussion: There may be lack of awareness in the CNA community that they can request a CVE ID for an AI/ML vulnerability today. The CNA Rules update will include clarification (e.g., demonstrative ML examples); additionally, other communications should be used to make it known more publicly.
- Some CVEs have been issued in this space, e.g., CVE ID 2019-20634, which is related to cloning machine learning model.
- Guests were amenable to further collaboration.

Open Discussion

- Google's new automated AI-driven fuzzing project
  - Google has plans to automate CVE assignments using AI fuzzing.
  - The Secretariat will reach out to Google to ask if they would present to the Board on their research into AI-driven fuzzing to automate CVE assignments.

Review of Action Items

None.

Next CVE Board Meetings

- 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)
- Wednesday, October 25, 2023, 9:00am – 11:00am (EDT)
- Wednesday, November 8, 2023, 2:00pm – 4:00pm (EST)
- Wednesday, November 22, 2023, 9:00am – 11:00am (EST)

Discussion Topics for Future Meetings

- Sneak peak/review of annual report template SPWG is working on
- 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