CVE Board Meeting Notes

April 12, 2023 (9:00 am – 11:00 am EDT)

Agenda

- 9:00-9:05 Introduction
- 9:05-10:25 Topics
  - Relationship between Vendor CNAs and Bug Bounty CNAs: Scopes and Policies
  - Update CISA ICS Scope to include U.S. Federal Enterprise
  - Potential Impacts of Pending Twitter API Changes
  - CVE Board Meeting during RSA
- 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
04.12.01	**Reach out to Twitter to see if there is an exception to allow FFRDC/government to stay with a non-paid plan, even with high volume tweets.**	**Secretariat**	
04.12.02	**Need to start planning for 2024 Summit.**	**Secretariat**	
04.12.03	**Review priorities list and assign responsible parties.**	**SPWG Chair**	

Introductory Remarks

- The CVE Project Lead is out sick and there is not yet an expected date of return.
- To keep CVE moving forward, an Acting Project Lead has been assigned. This person leads the Common Weakness Enumeration (CWE) project and has worked closely with CVE over many years.

Relationship between Vendor CNAs and Bug Bounty CNAs: Scopes and Policies

- A Board member noticed a URL in a disclosure policy for a CNA vendor that goes to a bug bounty site as opposed to the CNA's site.
- CNAs may leverage bug bounty services.
- Need clarity around who is assigning CVE IDs. Is it the CNA or the bug bounty organization?
- What do others think about the idea of assuring that CNAs have URLs that use the CNA's domains?
  - If a vendor CNA outsources to a bug bounty provider, the disclosure policy on the bug bounty site/domain must be clear that it's the CNA's policy.
  - A bug bounty organization cannot assign/publish CVEs unless they are also a CNA.

    - The CNA Rules can help clarify the relationship between CNAs and bug bounty organizations. Send recommendations to the SPWG.
    - Recommendation made to distinguish between bug bounty providers and non-providers.

Update CISA ICS Scope to include the Federal Enterprise

- A recent event with US federal PIV cards showed the need for a focus on vulnerabilities in the US federal enterprise space.
- Should we create a new CNA for this or expand CISA ICS scope to add federal enterprise? Current CISA scope is industrial control systems and medical devices.
- There were no objections to allowing CISA ICS to expand its scope to include federal enterprise vulnerabilities. The scope will be made clear that is only for US federal.
- The idea to rename CISA ICS to just CISA was discussed, but no decision was made.

Potential Impacts of Pending Twitter API Changes

- The CVE Program uses Twitter to share two types of information: Every time a CVE is published, and regular announcements like new CNAs.
- It is possible the CVE Program will be cut off because the current plan is a free one and it is unclear if there will be any notice before a cut off. There may be a need to transition to a paid account to stay on Twitter. There are also other information sharing options, e.g., Mastodon.
- Board input:
    - May still have some marketing value to some users, but there are other options. Would not pay a lot to stay with Twitter.
    - Reach out to Twitter to see if there is an exception for non-profit.

CVE Board Meeting during RSA

- The Board meeting on April 26 is the same week as RSA. Should the meeting be cancelled?
- It was agreed to move the meeting to the following week on May 3, and get back on the normal cycle with the May 10 meeting.

Open Discussion

- How is hard deploy going?
    - Bulk download is being used, and we have received feedback on some issues. As of last Friday, we feel that most of those issues have been addressed.
    - Next big rocks for the AWG are the ADP pilot and the user registry requirements.
- 2023 Priorities
    - Need to work on the data model for the user registry.
    - Staffing allocations for the user registry effort will be made in the new period of performance, which should start next week.

Review of Action Items

- 03.29.02 (JSON 4 deprecation). The secretariat is working with TWG on draft communication.
- 05.11.03 (Repo rules document). Slack may be serving the purpose.
- 07.06.01 (Update the FAQ section of cve.org). Secretariat will review the FAQ section to make sure there is no incorrect information.

- 06.23.01 (Program Annual Report). Need to start working on the outline now--set up sub WG to assist in building strawman.

Next CVE Board Meetings

- Wednesday, May 3, 2023, 2:00pm – 4:00pm (EDT)
- Wednesday, May 10, 2023, 9:00am – 11:00am (EDT)
- Wednesday, May 24, 2023, 2:00pm – 4:00pm (EDT)
- Wednesday, June 7, 2023, 9:00am – 11:00am (EDT)
- Wednesday, June 21, 2023, 2:00pm – 4:00pm (EDT)
- Wednesday, July 5, 2023, 9:00am – 11:00am (EDT)

Discussion Topics for Future Meetings

- 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, next is May 3, 2023)
- Council of Roots meeting highlights (next is May 3, 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