CVE Board Meeting Notes

April 3, 2024 (9:00 am – 11:00 am EDT)

Agenda

- Introduction
- Topics
  - Legacy File Deprecation and Question on CSV Support
  - VulnCon
  - CVE Game Plan for NVD Lull
  - Guest Speaker from CISA: Understanding Open Source in a CVE Context
  - Board Nomination and Vote
- Open Discussion
- Review of Action Items
- Closing Remarks

New Action Items from Today's Meeting

New Action Item	Responsible Party
None	

Legacy File Deprecation and Question on CSV Support

- The CVE Program will set up a discussion with DISA regarding the scheduled deprecation of the legacy CVE CSV download format and short and long term needs of stakeholders
- Concurrent with the ongoing discussions with downstream consumers, the CVE Program (via the QWG) will look at options for converting the current CVE Record Format (CVE JSON v5.x) to CSV in anticipation of either producing a download CVS file, or providing guidance for those users who will need to convert to CSV locally

VulnCon

- The Board had a hotwash after the inaugural VulnCon conference, but not all Board members were able to attend—just wanted to give those Board members an opportunity to give their perspective on VulnCon
  - Board member comments:
    - Loved VulnCon; have some notes written down and will send to VCEWG Chairs
    - Most interesting talk was one about data quality; a strategic imperative for the CVE Program is to improve data quality, which is difficult to do. (Discussion on data quality continues under next topic)
    - Coming out of VulnCon, we have a pretty good idea of a tiered approach that could be used (within the QWG) to improve data quality and a framework for how to prioritize data within the schema.
    - Need to be careful about not making the process (of improving data quality) too onerous for volunteer participants

CVE Game Plan for NVD Lull

- The CVE Program will be reaching out to CNAs (top 10 code-owning CNAs by number of publications) to make sure that they are aware that they can submit enriched data (e.g., CPE, CWE, CVSS) directly to the CVE Program, rather than submitting separately to the NVD.

    - Preliminary plan is for the CVE Program to offer to meet with the Top 10 by April 15 to discuss how those CNAs can add the optional data to their records.
    - The Secretariat will review CVMap to determine what data the Top 10 are providing to NVD; the program can figure out how to help those that are not providing any data
- Additionally, the CVE Program will host podcasts, create blog posts, etc., to explain this to the community.
- Board member comments:
    - CVE Program is in the position to take this enriched data from willing providers, so we need to let everyone know
    - Some CNAs may have enriched data that they could provide but do not realize that the program is able to ingest it
    - We have to roll back some legacy methods of submitting data to the CVE Program and NVD—CNAs may not realize they can submit it all to CVE Program via JSON 5.1 and then that data will roll into the NVD
    - There is an opportunity here for expanded federation with regards to enriched data. We need this to catch fire in the ecosystem and it starts with the CVE Program asking for it and we can determine who is willing and able to provide it. We can work with those willing but not able to help them provide it.
    - CVE Program may begin some sort of recognition incentive for those providing enriched data
    - Any organization that can provide enriched data to a CVE Record should do so as an ADP
    - Downstream consumers can decide for themselves what data they want to consume and what they do not care about
    - No need to accept all ADP results; consumers can choose to ignore what they want
    - If ADP functionality is out there and real, that functionality should include adding enriched data
    - Secretariat reference ADP will be ready to go by end of May
    - CVE Program will be able to support a production environment for the CISA ADP by end of April (that is not to say that CISA will go into production at that time)
- No Board members voiced disagreement with the approach to contact the Top 10 CNAs to ask them to submit enriched data directly to the CVE Program via JSON 5.1

Guest Speaker from CISA: Understanding Open Source in a CVE Context

- CVE Program has struggled with Open Source (O/S)
- CVE Project Leader asked the guest speaker from CISA weeks ago if there was a willingness to come and talk to the CVE Board about this topic—so they are here today to provide their perspective on the topic
- The guest speaker from CISA presented slides from their perspective and stated that we need to re-think the current model of the data model and process model for open source in a global context.
- Comments from Board members:
    - New guidance in the new rules may help mitigate the problem; I share your concerns with O/S CNAs coming online will put pressure on things. Numbers will be higher…but we still need IDs on these things. The answer does not seem to be fewer CVEs.
    - How does the CVE Program not collapse under the weight of exponential growth due to O/S?
    - The European Cyber Resilience Act (CRA)—is happening. It's a law. This will mean any commercial software sold in the EU will need a mark on it (self-certify) and will require things like CVEs, etc.

Board Nomination and Vote

- Two Board members met with a Board nominee at VulnCon last week and he voiced exasperation at the way the Board is handling his candidacy. They explained what was going on. The Board members asked if he'd be willing to go through an up/down vote as an individual board member even though he may lose, and the Board nominee indicated he wanted that vote.
- If we decide to move forward with the org liaison kind of position, if this Board nominee gets voted down as an individual board member, he should not have to wait the year before he can run for an org position.
- The org position is a different entity, and one vote does not have anything to do with the other
- Motion: Give the Board nominee an up/down vote as individual board member.
    - Using the "raise your hand" feature in Teams, the Board participated in a vote. Raise your hand if you agree with the up/down vote.
    - 12 of 12 Board members in the meeting agree to go forward with a vote

Open Discussion

- Board members asked if there is an easy way for a vulnerability reporter to know which CNA owns which product.
- There is not an easy way—this is a good use case for having a product registry
- Some CNAs include all covered products within their scope statement
- Some Board members agreed to meet offline to further discuss this topic

Review of Action Items

Out of time.

Next CVE Board Meetings

- Wednesday, April 3, 2024, 9:00am – 11:00am (EDT)
- Wednesday, April 17, 2024, 2:00pm – 4:00pm (EDT)
- Wednesday, May 1, 2024, 9:00am – 11:00am (EDT)
- Wednesday, May 15, 2024, 2:00pm – 4:00pm (EDT)
- Wednesday, May 29, 2024, 9:00am – 11:00am (EDT)
- Wednesday, June 12, 2024, 2:00pm – 4:00pm (EDT)

Discussion Topics for Future Meetings

- End user working group write-up discussion
- Board discussions and voting process
- ADP discussion
- Sneak peek/review of annual report template SPWG is working on
- Bulk download response from community about Reserved IDs
- 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