



CVE Board Meeting Notes

August 21, 2024 (9:00 am – 11:00 am EDT)

Agenda

- Introduction
- Topics
 - Summary of CPE and ADP/VEX Topics: QWG/SPWG
 - CVE Document Repository
 - CVE and AI Issues
 - Fall Technical Summit
- Review of Action Items
- Closing Remarks

New Action Items from Today's Meeting

New Action Item	Responsible Party
CPE Support: Identify a few people familiar with the subject that could potentially help with the problem and working a solution.	VCEWG Chair
CPE Support: Present CPE Support slide deck to QWG and following discussion bring back to CVE Board to make a decision.	QWG Chair
CVE Document Repository: Add “policy” to the readme on GitHub for this document repository and suggest changes to the “About” blurb.	Secretariat
CVE AI WG: Send calendar invite for CVE AI WG to all members of the Board.	Secretariat
CVE AI WG: Draft charter for the CVE AI WG and present to the Board for official discussion and vote.	CVE AI WG Member
CVE Fall Summit: Review calendars for availability on October 15 th or October 22 nd .	CVE Board
CVE Fall Summit: Send out a save the date and start creating Summit website.	Secretariat/CVE Board
Schedule QWG meetings weekly instead of biweekly.	Secretariat

Topics

Summary of CPE and ADP/VEX Topics: QWG/SPWG

- Technical discussion in QWG and SPWG about CPE and its role in enrichment and how it could be incorporated into the CVE Record in a more usable way than what we currently have. There could be better ways of defining it and allowing consumers of CVE records to understand and better interpret what we mean when we have CPEs.
- We need to make some schema updates to better support CPEs and we need to guide producers of the records in a more consistent way of defining CPEs.
- Slides with examples of the potential solutions proposed for CPE in CVE Record Format were presented.
 - **ACTION: Identify a few people to invite to help with the problem and work the solution for CPE support.**
 - Possible Solutions and Proposals
 - Solution 1.1: Documentation and guidance – enforce cpes array to contain only affected CPE Names
 - Solution 1.2: Documentation and guidance – enforce cpes array CPE Names to match versions status property.

- Solution 1.3: Documentation and guidance – enforce cpes array contain only a CPE Match String without version.
- Solution 2: Rename cpes array to affected-cpes array, create new arrays for unaffected-cpes and unknown-cpes.
- Solution 3: Move cpes array down a level to the version block
- Solution 4: Change cpes array to be array of objects instead of array of CPE strings.
- Solution 5: Implement NIST NVC CVE configurations block within CNA and ADP containers

- Will continue the discussion in the QWG

CVE Document Repository

- There's a set of documents that are important enough policy, rules, and guidance documents that they must be decided by board vote.
- Suggestion was to track the changes transparently using GitHub. Goal was to turn a PDF into a clean markdown.
- The idea moving forward is when the board votes on changes within a document, you could come into the repo on GitHub and see a pull request with changes in it that would get approved and then there would be a history of changes within the document over time.
- Board Discussion
 - A useful GitHub feature here could be the code owners feature, where you can define a code owners file, which can either be individuals or a team that is responsible for various locations within the repo, and you can combine that with the review feature to basically force certain people to review certain things. That could be a way for us to ensure that various working groups have an opportunity to weigh in on specific changes before they are permanently made.
 - With privileges, it may fall to the Secretariat to make any further changes to the repo, as well as any next steps decided.
 - Change CVE Documents heading to CVE Policy Documents as the purpose of this was to identify those documents that require a board vote for any changes. This is not open season on these documents and we're not allowing anyone to change these documents. This is going to be by the board itself, so I would change the title and the descriptions that talk about CVE policy documents because that is truly what this is about.
 - **ACTION: Add "policy" to the readme on GitHub for this document repository and suggest changes to the "About" blurb.**
- At the very minimum, use this to keep track of changes.
- We also want to be careful that we don't have accidental translation formatting errors that pop in.
- Maintenance of this GitHub repo will continue as documents are added/changed.

CVE and AI Issues

- There was a published blog on the subject, which was intended to be a series of blogs publishing CVE's position with respect to AI related vulnerabilities and what is in and out of scope, as well as the guardrails for where the community should go for certain types of problems.
- The CVE AI WG is currently working on the guardrails definition and where these lines are. It was proposed at the last meeting that we continue to gather some examples of cases that are being brought to the purview of various CNAs and the CNA-LRs. The CNA- LRs are getting some repeated types of questions and having these case studies is a great way to build up toward guardrail policy.
- Next goal for the CVE AI WG is to publish a second blog, but we're not ready for that yet and need the Board's help to work on that.
- Four topics that the WG is currently looking at:
 - AI Tools
 - We are familiar with how to manage vulnerabilities from tools and if a particular AI product has a vulnerability, that is straightforward.
 - AI Report Quality
 - If an AI product gives us poor quality output and results, is that a vulnerability or not? Is it worthy of a CVE entry or not?
 - AI Implementation

- If a particular product is trained on medical conditions, for example, and a particular organization applies that same AI product to business situations, the AI is going to produce poor results because it was trained on one domain and is now being used for another domain. Is that worthy of a CVE vulnerability?
- AI Service Versioning
 - There may be situations where there's a particular exploit available, even publicly happening out in the world, but AI services are being updated very frequently, often daily, sometimes more often than the daily. The question is how do we manage versioning when these AI products and services are continually changing?
- Some of these topics fall within the scope of similar activities we have with cloud services, especially the last one, so I think with some of those discussions, we need to try to equate them to what we're already doing and go from there.
- Important to provide continuing education to the Board for future decisions on guidelines.
- Board Discussion
 - Everyone on the Board should be invited to this AI WG.
 - Isn't the Board supposed to vote on the formation of working groups? Did this come to the Board for a vote? Also supposed to have a charter for the Board to review before voting on WG formation.
 - Yes, the Board does need to vote on WG formations.
 - It was originally just going to be a couple of out-of-cycle meetings to discuss the deep dive that we went through after VulCon and, as things happen in AI, they started to evolve into a bigger discussion with an active meeting on the calendar. This was an organic kind of situation and now it's worth considering a working group and if you want to make a requirement right, make a request and we can do that.
 - **ACTION: Draft a charter for the CVE AI WG and present to the Board for discussion and an official vote.**

Fall Technical Summit

- Envisioned as one day, unless we have topics that exceed that. It will be a virtual event requiring help from the Secretariat and the Board.
 - Based on topics discussed during the meeting, we may need a day and a half to cover topics and there was a suggestion to have multi-tracks.
- There are two potential dates: October 15th and October 22nd. Are there other dates to consider in the middle of November?
 - **ACTION: Review calendars and see if either of these dates work for Board members.**
- **ACTION: Work with the Secretariat to send out a save date and start setting up a webpage.**
- Continue discussion at next CVE Board meeting.

Review of Action Items

- None.

Next CVE Board Meetings

- Wednesday, September 4, 2024, 2:00pm – 4:00pm (EDT) – Working Group Updates
- Wednesday, September 18, 2024, 9:00am – 11:00am (EDT)
- Wednesday, October 2, 2024, 2:00pm – 4:00pm (EDT) – Working Group Updates
- Wednesday, October 16, 2024, 9:00am – 11:00am (EDT)
- Wednesday, October 30, 2024, 2:00pm – 4:00pm (EDT) – Working Group Updates
- Wednesday, November 13, 2024, 9:00am – 11:00am (EDT)

Discussion Topics for Future Meetings

***Bold items are those flagged for discussion need.**

- 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
 - Should be an action item not future discussion topic.
- Secretariat review of all CNA scope statements
- Proposed vote to allow CNAs to assign for insecure default configurations
- CVE Communications Strategy