CVE Board Meeting Notes

September 28, 2022 (9:00 am – 11:00 am ET)

Agenda

- 9:00-9:05 Introduction
- 9:05-10:25 Topics
  - Working Group Updates
  - CVE Services Deployment Go/No Go
  - Dispute Policy Vote
- 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
09.28.01	Email to Board list to request yes/no vote on the October 3 soft deploy.	Secretariat	
09.28.02	Email to Board list about potential removal of inactive board members. Discussion/vote on removal at next Board meeting.	Secretariat	
09.28.03	Distribute Doodle Poll to Board members to select a date/time for an interview with a candidate Board member.	Secretariat	

Working Group Updates

- Automation Working Group (AWG)
  - The AWG made the unanimous (13-0) decision on September 27, to recommend soft deployment proceed as planned on October 3. This was based on scorecard results and communications/coordination with the Transition Working Group (TWG) and Quality Working Group (QWG).
  - The Deployment Recommendation slide deck was distributed to the Board and all working groups on September 27.
  - The Strategic Planning Working Group (SPWG) chair provided concurrence verbally on September 27 to proceed with deployment.
  - There are three remaining Git Hub/JSON 5.0 issues that the QWG does not think should delay an October 3 soft deployment.
  - Final testing of 'client zero' is happening this week. Any problems could result in a deployment delay.

- After Board approval, final concurrence by the Secretariat is needed to deploy.

- CNA Coordination Working Group (CNACWG)
  - Collaborating with the Outreach and Communications Working Group (OCWG) on a blog post about CVE and a podcast about the CNACWG mentoring program.
  - The AWG Chair asked how the AWG can best support the CNA community as they adopt CVE Services 2.1, as well as the Mentoring Program. Ideas were:
    - The Mentoring Program is currently using Google Sheets, but something more automated or with more features, would help.
    - Attend a CNACWG meeting and present abbreviated version of slides explaining the CVE Services 2.1 deployment and impact on CNAs. The AWG chair will attend next meeting, on October 5.
  - There are plenty of mentors who have volunteered in the new Mentorship Program
  - No noticeable themes have emerged from the mentoring sessions (e.g., common problems or questions from CNAs being mentored), and only a few issues have come up which were quickly addressed. If themes are noticed, let MITRE Top Level Root know so CNA onboarding can be improved.

- Transition Working Group (TWG)
  - Preparing for the upcoming CVE Services 2.1 Workshop on November 2.
  - Outlines of presentation topics, conformation of speakers, and expected time requirements are due September 29.
  - Top level outline:
    - Introduction: Brief and Recording
    - Introduction to JSON 5.0: Brief and Recording
    - JSON 5.0: Tips and Guidance
    - Transition Plan: Brief and Recording
    - CVE Record Workflow Tutorial: Brief and Recording
    - How to get a CVE Services Account: Brief and Recording
    - Red Hat Client Tutorial: Readme file, Brief and Recording
    - Vulnogram Tutorial: Readme file, Brief and Recording
    - CVEClient Tutorial: Readme file, Brief and Recording

CVE Services Deployment Go/No Go

- A presentation was provided to explain why the AWG recommends CVE Services 2.1 soft deployment begin October 3.
- Current deployment scorecard results show eight out of nine scorecard topics are Green (ready to go). One Yellow remains for CVE Services Testing: Integration Testing (Secretariat).
  - User Stories Complete (Green)
    - 44 GitHub Issues/Users Stories for the CVE Services/Record Submission and Upload Service (RSUS)
      - 25 Stories completed.
      - 9 Stories recorded as OBE/Invalidated based on AWG Discussions.

        - 5 “Secretariat only” implementations business requirements discussed with TWG. An interface/API for the general public to allow searches of CVE Records is costly, so for now keep at Secretariat-only level.
        - 5 Stories deferred based on AWG discussion and board discussion (re: related to ADP, tweeting, and logging history).
    - Unit Testing Complete (Green)
        - All tests were run and passed.
    - CVE Services Testing (unscored)
        - Functional testing (Green): Performed by the development team (interfaces tested per role, and documentation posted to Swagger) and the user community)
        - Integration testing (Yellow): Two phases – Automated Testing is done, and MITRE CPS (client zero) Interface Human Testing is on-going and expected to complete this week.
    - Client Preparation (Green)
        - Three clients: Cvelib (ongoing testing with positive results so far, CVE Services 2.1 compliant); cveClient (tested and shown to be compliant with CVE Services 2.1); and Vulnogram (tested and shown to be compliant with CVE Services 2.1).
    - Roll-out Plan (Secretariat) (Green)
        - Deployment Strategy (soft deploy and hard deploy)
        - Communication Strategy (three distinct audiences, message/content, methods – bulletins, email, Slack, YouTube)
        - Deployment Procedures (e.g., back up procedures, scripting/procedures for JSON 4.0 to JSON 5.0 conversion, importing upconverted data, roll-back procedures)
    - Security Evaluation (Green)
        - Security policy being enforced at each of the CVE Services APIs (defined in SWAGGER documentation).
        - Secure code review (internal team) issues have been resolved.
        - Security architecture/threat model review conducted by Red Hat. All high and critical issues have been resolved. Remaining low issues to be addressed later.
        - Penetration testing conducted by the community and Secretariat identified high and low priority issues. All high priority issues have been resolved.
    - CVE Services 2.1 Roll-back Plan (Green)
        - Timeline of the roll-back window (and steps to ensure no data are lost), and a cut-off date for when a roll-back can occur.
    - Contingency Planning/Technical Support (Green)
        - Discussion about plans for user technical support (Slack is preferred, but web form can also be used) and operations support (MITRE Operations Center), if bugs or issues occur in production.
        - Does not include client debugging.
    - CVE Services Workshop Training Preparation (Green)
        - Topics and content requirements are well understood.
        - A date and agenda are set.
        - Briefing outlines from presenters are due September 29.
- A meeting goal was to conduct a Go/No Go vote for Soft Deploy on October 3.
    - A Board quorum was not present. Of those in attendance at the time of the vote, the vote was 10-0 in favor of starting Soft Deploy on October 3.

- Next steps: Make the meeting recording available on the CVE Program private YouTube site, send an email to the Board with guidance how to access the recording, request their vote if they were absent from the meeting.

Dispute Policy Vote

- The Record Dispute Policy was distributed to the Board for approval on September 21, with a due date for September 28 for responses.
- Sixteen Board members voted Yes, and none voted No.
- The policy has been posted to the CVE Program website here.

Open Discussion

- What is the status of the check-in with absent/inactive Board members?
  - One member resigned.
  - Another had feedback that Board meetings are too operationally or tactically focused to justify attendance.
  - Others have not responded to initial attempts to reach them. Another attempt to contact will be made. Next step is for the Board to decide status.
- Comment that additional communication with the Board encouraging attendance at today's meeting would have been helpful, given that an important vote was planned about the October 3 Soft Deployment. Feedback accepted; program will work to improve.
- Is it okay to use Doodle Poll to select an interview time for a candidate Board member?
  - Doodle is fine in a case like this. It cannot be used for official Board votes.
- What is the status of the reach out to a prospective Board member?
  - Contact has been made and there is interest. There will be some delay in next steps as the candidate makes a job transition.
- What are Board reactions to the feedback that meetings can be too tactical?
  - The Board's normal focus is strategic, but there are times when significant changes are required, and these require the Board's understanding. In these cases, Board meetings may be more tactically focused.
  - Comment to try to do more things via the Board email list, and use Board meetings for questions, concerns, etc. Recent participation using the list has been lighter than earlier in the program, and this may be a result of the increased frequency of Board meetings since then.

Review of Action Items

- 09.30.04: Dispute Policy is approved. Status changed to Complete.
- No updates to other action items.

Next CVE Board Meetings

- Wednesday, October 12, 2022, 2:00pm – 4:00pm (ET)
- Wednesday, October 26, 2022, 9:00am – 11:00am (ET)
- Wednesday, November 9, 2022, 2:00pm – 4:00pm (ET)
- Wednesday, November 23, 2022, 9:00am – 11:00am (ET)
- Wednesday, December 7, 2022, 2:00pm – 4:00pm (ET)
- Wednesday, December 21, 2022, 9:00am – 11:00am (ET)

Discussion Topics for Future Meetings

- Removal of inactive Board members
- CVE Services 2.1 and CVE Program website transition updates (on-going)
- Summit planning updates
- Working Group updates, every other meeting
- Council of Roots meeting highlights (on-going)
- Researcher Working Group proposal for Board review
- Vision Paper and Annual Report
- Initiate Board vote for a proposed solution to allow CNAs to assign IDs for insecure default configuration (from closed action item 03.03.02)
- Resolution on the breakout thread about the year notation in CVE IDs (in-progress)