CVE Board Meeting Notes
March 30, 2022 (2:00 pm – 4:00 pm ET)

CVE Board Attendance

☐Ken Armstrong, EWA-Canada, An Intertek Company

☒Tod Beardsley, Rapid7

☐Chris Coffin (MITRE At-Large), The MITRE Corporation

☐Jessica Colvin

☐Mark Cox, Red Hat, Inc.

☐William Cox, Synopsys, Inc.

☒Patrick Emsweller, Cisco Systems, Inc.

☐Jay Gazlay, Cybersecurity and Infrastructure Security Agency (CISA)

☐Tim Keanini, Cisco Systems, Inc.

☒Kent Landfield, Trellix

☒Scott Lawler, LP3

☒Chris Levendis (MITRE, Board Moderator), CVE Program

☒Art Manion, CERT/CC (Software Engineering Institute, Carnegie Mellon University)

☐Pascal Meunier, CERIAS/Purdue University

☐Ken Munro, Pen Test Partners LLP

☐Tom Millar, Cybersecurity and Infrastructure Security Agency (CISA)

☒Chandan Nandakumaraiah, Palo Alto Networks

☐Kathleen Noble, Intel Corporation

☒Lisa Olson, Microsoft

☒Shannon Sabens, CrowdStrike

☒Takayuki Uchiyama, Panasonic Corporation

☒David Waltermire, National Institute of Standards and Technology (NIST)

☐James "Ken" Williams, Broadcom Inc.

MITRE CVE Team Attendance

☒ Kris Britton

☒ Christine Deal

☒ Dave Morse

☒ Art Rich

Agenda

- 2:00-2:05   Introduction
- 2:05-3:35   Topics
  - Working Group Updates
  - Open Discussion
- 3:35-3:55   Review of Action Items
- 3:55-4:00   Next Meetings and Future Agenda Topics

New Action Items from Today's Meeting

Action Item #	New Action Item	Responsible Party	Due
	none		

Working Group Updates

- Automation Working Group (AWG) (Kris Britton)

  – CVE Services 2.1 entered community penetration testing on February 25 (ZDI, RedHat, Rapid7, Secretariat provided findings)

  – There are 45 findings with various levels of difficulty to correct. 23 of the findings require fixing prior to the 2.1 release.

  – Two-week sprints are planned to fix the problems. Sprint 1 is underway and scheduled to complete April 1

  – A schedule update is in-progress to reflect the impact of the sprints on the release date. Summit rescheduling cannot happen without more clarity about when Services 2.1 will be operational.

  – AWG is also working on documentation needed to operate and maintain Services 2.1.

  – ADP requirements are on the "back burner" for a while due to other priorities.

- Quality Working Group (QWG) (Dave Waltermire)

  – The group has received feedback on the JSON 5 record format, and they are working on adjustments/tweaks to the format.

  – They are also working with Joe Whitmore and the development team on content conversion from JSON 4 to 5. QWG is reviewing converted records and providing feedback.

  – Dave and Chandan are planning to step down as co-chairs when a suitable replacement can be identified. Their shifting priorities are making it difficult to keep up with QWG administration (e.g., meeting logistics, notes and distribution, handling GitHub issues, and documentation development). An estimate of time commitment is 4 hours/week.

- Strategic Planning Working Group (SPWG) (Kent Landfield)

- Kent mentioned he needs a co-chair; Chris Levendis volunteered help out as needed, at least in the near-term.
- CVE Services 2.1 delays are causing a delay to the ADP pilots.
- The CVE Working Group Operations Handbook is out for final review, awaiting feedback.
- For disputed tagging, more clarity is needed about how to use it. Kent and Dave Waltermire to get together to discuss.
- The question was asked if it would be helpful for all WG chairs to attend the SPWG meeting. The answer was yes, it would be fine if you have the bandwidth, but bring your priorities. Chairs can also be invited on an as-needed basis for a particular topic.

- Outreach and Communications Working Group (OCWG) (Shannon Sabens)
  - Shannon mentioned she needs a co-chair. A current working group member has been approached with the offer, but no decision has been made yet.
  - There is an interest in better communications and outreach with Researchers. A podcast focused on Researchers is in-progress, with an estimated mid-April target date. Shannon and Bob Roberge are working on message content. A key idea is to get away from a CNA focus, and instead focus on Researchers and how they communicate and relate to a CNA partner. This may evolve into a series of podcasts.
  - The CNA Newsletter went out March 28.

- CNA Coordination Working Group (CNACWG) (Tod Beardsley)
  - The CNACWG meetings no longer include a European time zone occurrence, due to lack of interest. European members are fine with the US time zone occurrence.
  - The group is working on an idea to create a voluntary CNA mentoring program. This would augment on-boarding orientation sessions and could help bring new CNAs up to speed faster.
  - A related idea is to send out a periodic survey (e.g., quarterly) to ask new CNAs (3-6 months into the program) what they liked about on-boarding and what would have been nice to know.
  - The mentoring program would follow a big brother/big sister model where an experienced CNA pairs up with a new CNA to help the new CNA understand, for example, such activities as ID assignment and CVE Record publishing/submission. This is not intended to be a heavy time commitment – maybe 4 hours per month. It could also be an opportunity to encourage new CNAs to be active in the program working groups. An understanding of which CNAs have completed their registration and are in the pipeline would be helpful to target who needs mentoring. It will probably take at least two more CNACWG meeting cycles to get a proposal ready for Secretariat involvement/review.

- Transition Working Group (TWG) (Lisa Olson)
  - Lisa brought up the idea of having a face-to-face meeting with the TWG members (all the working group chairs) to discuss the "next big things coming up." Other Board

members could attend at their option. A one hour per week meeting is not enough time to address all the important things going on right now. Travel was mentioned as a concern, so maybe a 3-hour conference call would be better. This will be discussed further at the TWG meeting tomorrow.

– It was suggested to reframe the Summit as a workshop to get familiar with the new CVE services. Should include demos, hands-on exercises, etc.

Open Discussion

▪ Possible New Researcher Working Group

– As a follow-on to the OCWG update, Chris Levendis reminded everyone that the idea of a new researcher working group is still under consideration, and a proposal is being worked on for Board review.

– The idea is to provide a forum (not just social media) where Researchers and the program can collaborate, share concerns, ask questions, etc.

– There was some discussion about whether to call it a working group or something else that has a more project-oriented connotation (e.g., advisory committee, special interest group, etc.).

▪ Council of Roots Meeting Highlights (held March 30, at 8:00 a.m. EDT)

– Timeframe for CVE Record Submission

▪ The CVE Record Submission timeline target is 5 business days. The topic was whether that should be changed.

▪ Feedback from the meeting indicated that Roots are familiar with the 5% Reserved but Public (RBP) threshold but are not aware of the 5-day best practice to submit a CVE Record. CNA on-boarding needs modification to better explain this.

▪ There was no objection to changing the 5-day submission from a best practice to a rule (include in the updated CNA Rules document, currently in review).

▪ The consensus was to leave the duration at 5 days, and after RSUS has been operational for a while, reevaluate.

▪ Board comments:
  • 5 days seems a bit long.
  • Automation will help when operational, in terms of speeding up the record publishing process.
  • With automation, 24 hours should be the goal.
  • Board is okay keeping at 5 days until automation is in place for a while.

– Reserved but Public (RBP) CVE IDs

▪ The RBP threshold is 5%, and the topic was whether that should be changed.

▪ Refers to a CVE ID that's been released to the public, for example in a product advisory, but is not yet available on the publicly facing CVE List.

- This creates confusion in the user community and results in the program having to field a lot of questions.
- Once the 5% threshold is met, a CNA cannot request any more CVE IDs until they work down their current IDs, or they can request a one-for-one swap.
- After enhanced automation is operational for a while, the program can evaluate whether an adjustment to the 5% threshold is needed. Automation is expected to make RBPs less of a problem.
- When CNAs request large blocks of CVE IDs, the program tells them we're transitioning away from that approach, and they can come back for more IDs over time, as needed.
- Roots agreed the program should keep the threshold at 5% for now, and then reevaluate after automation has been in place for a period of time.
    - Meeting Format
        - Roots liked the meeting agenda format, which was more focused on specific topics, and less focused on open discussion.
- Suggested Topics for Future Council of Roots Meetings?
    - The Board suggested that after SPWG puts together a general framework or model for dispute tagging, it can be handed off to the Roots so they can provide input on how best to operationalize it.

Review of Open Action Items

- None

Next CVE Board Meetings

- Wednesday, April 13, 2022, 9:00am – 11:00am (ET)
- Wednesday, April 27, 2022, 2:00pm – 4:00pm (ET)
- Wednesday, May 11, 2022, 9:00am – 11:00am (ET)
- Wednesday, May 25, 2022, 2:00pm – 4:00pm (ET)
- Wednesday, June 8, 2022, 9:00am – 11:00am (ET)

Discussion Topics for Future Meetings

- CVE Services updates, as needed
- CVE Program website transition progress, as needed
- Council of Roots meeting highlights
- Researcher Working Group proposal for Board review
- Vision Paper and Annual Report

CVE Board Recordings

The CVE Board meeting recording archives are in transition to a new platform. When the new platform is ready, recordings will be available to CVE Board Members. Until then, to obtain a recording of a CVE Board Meeting, please reach out to the CVE Program Secretariat (cve-prog-secretariat@mitre.org).