CVE Board Meeting Notes

July 20, 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)
☐Art Manion, CERT/CC (Software Engineering Institute, Carnegie Mellon University)
☐Pascal Meunier, CERIAS/Purdue University
☐Tom Millar, Cybersecurity and Infrastructure Security Agency (CISA)
☐Ken Munro, Pen Test Partners LLP
☐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
☐ Phil Taggart

Agenda

- 2:00-2:05 Introduction
- 2:05-3:35 Topics
    - CVE Program Documentation Updates
        - Working Group Operations Handbook
        - Program Governance and Organization
        - CNA Operational Rules
    - Identity Management for CNAs (i.e., Slack/Discord membership)
    - Art Manion Leaving CERT/CC
    - Open Discussion
- 3:35-3:55 Review of Action Items
- 3:55-4:00 Closing Remarks

New Action Items from Today's Meeting

Action Item #	New Action Item	Responsible Party	Due
	None.		

CVE Program Documentation Updates (Dave Morse)

- Working Group Operations Handbook
    - Distributed 6/22/22 and 7/6/22 to the Board for final review and in preparation for an approval vote. Some comments from Dave W have been received.
    - It was noted that the version should be v1.0, not v3.0. Earlier versions were never formally approved.
    - Additional comments from Kent were made (and will be provided) about:
        - Section 2 – CVE Program-supplied Collaboration Tools. Needs update to reflect current practices. Working Groups are using some non-MITRE-supplied tools.
        - Section 3.2 – Membership Size. Remove first bullet about insufficient resources. This has not been a problem to date.
        - Appendix A, Membership Size section. There is no need to specify a maximum number of members. There have been no problems to date.
    - Next steps
        - Comments will be consolidated and addressed where possible.
        - Questions that remain will be in comments.
        - Updated version will be sent to the Board via email.
        - Timing: no specific date, but provide the update at least one week prior to a Board meeting, to allow time for review and possible discussion at the upcoming meeting.

- It was agreed that, when the document is ready, a consensus vote (not a majority vote) will be used for approval. The document is a guide, not strict rules.

- Program Governance and Organization
  - No discussion today.
  - Distributed 6/24/22 to Board for initial review. No comments to date.
  - Agreed at 7/6 Board meeting to pause further review until the WG Handbook is approved.
- CNA Operational Rules
  - No discussion today.
  - Distributed 6/24/22 to the SPWG for initial review. No comments to date.
  - Agreed at 7/6 Board meeting to pause further review until the WG Handbook is approved.
  - SPWG plans to have a new meeting schedule out soon. This document will be an early topic for the group.
  - Finalization has a dependency on CVE Services implementation.
  - Order of review will be SPWG, CNACWG, and the Board.

Identity Management for CNAs (Tod Beardsley)

- With an increasing number of CNAs, identity management of CNA representatives will become increasingly important.
- There is no current way to tell who a CNA representative is for a given CNA without reaching out to the Secretariat. This can lead to difficulties joining Slack or Discord communities, Working Groups with restricted memberships, and other lists, as the number of CNAs grows.
- Is this a problem we can solve?
  - The program had a design for a user registry that was intended to solve this problem.
  - CVE Services 2.1 will have functionality to allow a user to query whether a particular person is associated with a CNA.
- Gradations of access control for CVE Services will be needed, particularly with a growing number of external interface requirements. This should not be a priority right now, however.

Art Manion Leaving CERT/CC (Dave Morse)

- Art plans to remain on the Board.
- Board membership is an individual membership, not organizational.

Open Discussion

- VulDB
  - VulDB is a CNA that has issued CVE IDs for vulnerabilities outside its scope.
  - An initial call with the program and VulDB was positive.
  - Follow up email from CNA expressed interest in Trusted Researcher pilot and proposed ideas for future efforts.
  - **The email will be shared with the Board** via the eBoard list, so there can be open and transparent discussion.

- CNAs cannot prevent a CVE ID from being issued. They have right of first refusal, but the CNA-LR may decide to issue.

- Dispute Policy
  - Draft was sent to the Council of Roots on 7/19 for a two week review period.
  - **The draft will be forwarded to the Board** for their review.

- Council of Roots Meeting
  - The Board would like updates from the monthly Roots meeting.
  - Meeting highlights will be an agenda topic for the next Board meeting.

- CVE ID Year Notation
  - Brought up at 6/22/22 meeting. There is confusion in the CVE community about what the "year" in the CVE ID means. It is currently undefined.
  - Clarification will be provided in the updated CNA Operational Rules.

- Cloud-based Vulnerabilities
  - Microsoft has received questions recently about cloud-based vulnerabilities.
  - They are currently working on a blog to explain their policy, and plan to have the blog posted next week. When posted, it will be provided (link) to the Board.
  - CNA Operational Rules need to provide clarification about cloud-based vulnerabilities.
  - Chris Levendis has an action to also develop a blog to explain program policy about cloud-based vulnerabilities.
  - Blog/policy language should be finalized first, then Rules updates can happen.

Review of Action Items

No new updates.

Next CVE Board Meetings

- Wednesday, August 3, 2022, 9:00am – 11:00am (ET)
- Wednesday, August 17, 2022, 2:00pm – 4:00pm (ET)
- Wednesday, August 31, 2022, 9:00am – 11:00am (ET)
- Wednesday, September 14, 2022, 2:00pm – 4:00pm (ET)
- Wednesday, September 28, 2022, 9:00am – 11:00am (ET)

Discussion Topics for Future Meetings

- CVE Services 2.1 and CVE Program website transition updates (on-going)
- Summit planning updates
- Working Group updates, every other meeting (next scheduled for August 3)
- 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 (Tod B) (in-progress)