CVE Board Meeting Notes
June 22, 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 ID Year Notation
    - Status Update on Program Documentation
    - 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 ID Year Notation

- An individual on Slack mentioned there is confusion about what the "year" in the CVE ID means. The meaning of the year is currently undefined.
- Tod B drafted and shared explanatory text with the CNACWG that can be included in the CNA Rules document. The text was also shared at the Board meeting (perhaps add to section 5.1.6 of CNA Rules v3.0).
    - *"MUST maintain the CVE ID syntax (e.g., CVE dash year dash arbitrary number of digits).*
        - *The year part SHOULD be the year the CVE ID is reserved, and SHOULD indicate the approximate year of the public disclosure of that vulnerability.*
        - *The year part MAY be the year the vulnerability was disclosed if the vulnerability was disclosed in the past.*
        - *The year part SHOULD NOT be in the future at the time of the CVE ID reservation."*
            - The key part of this is SHOULD NOT – it's common to reserve IDs late in a calendar year and not publish the associated record until the following calendar year.
- This draft text will be reviewed/revised and added to the CNA Rules update.
- The year can be interpreted as the year discovered, the year a CVE ID was assigned, or the year the CVE Record was published. The Rules need to make clear.
- Next steps: Tod will post the draft text to the thread and ask for comments. The updated rule wording may be ready for a vote at the next Board meeting.

Status Update on Program Documentation

- CVE Working Group Operations Handbook
    - Draft update of v2.0 to v3.0.
    - Distribute to Board for review after this meeting, and discuss comments/issues at next meeting. Ask for confirmation that reviewers read the document.
    - Board vote of approval will occur via the mailing list, not during a Board meeting.

- CVE Program Governance and Organization
    - Initial version 1.0 (draft).
    - Send out again for review and discuss comments/issues at next Board meeting. Ask for confirmation that reviewers read the document.
    - Comments received will determine next steps (more work needed or ready for vote).
    - Board vote of approval will occur via the mailing list, not during a Board meeting.
- CVE CNA Operational Rules
    - Draft update of v3.0 to v4.0.
    - Finalization is dependent on resolution of existing comments and operational changes due to CVE Services 2.1.
    - SPWG will provide the first review, followed by the CNA community. Any CNA-suggested updates will be made and SPWG will perform another review, prior to presenting an update approval to the Board.

Open Discussion

- Would be helpful to have a periodic debrief from the Transition Working Group periodically at Board meetings to keep everyone up to date about CVE Services status. This will happen at the next Board meeting with the regular WG update cycle (every other meeting).
- At the Council of Roots meeting earlier today, a demo of Monday.com was provided, along with instructions how to get an account set up. Participation by Roots on Monday.com is light, and the program continues to encourage its use. A test board has been set up so Roots can practice using the tool to get comfortable.
- Topics for the next Board meeting should be: CVE Services and CVE Website transition updates, and WG highlights.

Review of Action Items

- 09.30.04 – QWG and SPWG to review after Secretariate review. Updated Dispute policy needs review prior to JSON 5.0 release with CVE Services 2.1.
- 10.26.01 – combine with 09.30.04.
- 10.28.01 – current draft version of WG handbook to be distributed to Board for review.
- 12.16.01 – keep separate from the WG handbook so no slow down getting the handbook out.
- 04.14.02 – address prior to summit (now called workshop). The workshop won't happen prior to mid September. Build guidance material for the workshop that can be used post-deployment and operations of CVE Services 2.1.
- 06.23.01 – Target end of January 2023 for 2022 report release.
- 10.26.02 – Tod to follow up.
- 10.26.03 – tabled in favor of the CNA mentoring program; move to Closed/OBE tab.
- 04.27.01 – blog examples have been forwarded to Art M. Move to Closed/OBE tab.
- 04.27.02 – Tod made initial contact with the journalist; no response yet. CNA Rules are not clear enough on handling cloud vulnerabilities.
- 05.11.02 – combine with 05.11.03 (regarding a program repository and associated rules document about how to use the repository).

Next CVE Board Meetings

- Wednesday, July 6, 2022, 9:00am – 11:00am (ET)
- Wednesday, July 20, 2022, 2:00pm – 4:00pm (ET)

- Wednesday, August 3, 2022, 9:00am – 11:00am (ET)
- Wednesday, August 17, 2022, 2:00pm – 4:00pm (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 July 6)
- 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)