CVE Board Meeting Notes
July 6, 2022 (9:00 am – 11:00 am 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
        - Governance and Organization
        - CNA Operational Rules
    - Working Group Updates, including CVE Services and CVE Website Transition Updates
    - VulDB Issue
    - 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
07.06.01	Update program FAQs on CVE.org	Chris L.	TBD

CVE Program Documentation Updates (Dave Morse)

- Working Group Handbook
    - Distributed 6/22 to Board for final review and in preparation for a vote. No comments to-date.
    - Some Board members indicated they could review the document later today.
    - The document will be sent out again, with a one-week review period. This will provide time to resolve comments prior to discussing the document at the next Board meeting on 7/20.
    - A Board vote (virtual) is expected soon after the 7/20 Board meeting.
- Program Governance and Organization
    - Distributed 6/24 to Board for initial review. No comments to-date.
    - There was consensus to pause further review until the WG Handbook is approved.
- CNA Operational Rules
    - Distributed 6/24 to the SPWG for initial review. No comments to-date.
    - Dependency on CVE Services implementation.
    - There was consensus to pause further review until the WG Handbook is approved.
    - Once restarted, the order of review will be SPWG, CNACWG, and the Board.

Working Group Updates

- SPWG (Kent Landfield)
    - Reactivation of SPWG meetings is planned for later this month.

- Members will be polled for meeting day and time preference, and a new meeting series will be created by the Secretariat.

- OCWG (Shannon Sabens)
  - Last few meetings have been lightly attended. Going forward, there is a change in the meeting schedule that may help. The main group meeting will now be on Tuesdays, and Shannon will also meet with Bob Roberge on Fridays.
  - Completed a podcast with Madison Oliver about removing the CVE stigma.
  - Working with Tod Beardsley to create content about the CNA Mentoring Program the CNACWG recently implemented.
  - Send topic ideas for future program blogs or podcasts to OCWG.
  - The observation was made about seeing negative media/press coverage that says CVE doesn't deal with cloud vulnerabilities. A blog should be written to explain that the program does deal with cloud vulnerabilities and provide an overview of the process. This is an existing Action Item (04.27.03) that Chris Levendis leads.
- QWG (Dave Waltermire)
  - Continuing to work through JSON 4 to JSON 5 content conversion issues. The four main ones are:
    - There are 490 CVE Records that are not on the GitHub CVE List, but are on CPS. Corrective action is in progress.
    - Working on refinements to the process to generate tags for references.
    - There are a few cases where converted records are empty. This is due to a glitch in the converter. Problem has been identified and the fix is in progress.
    - Working on a process to extract and preserve the 'date published' information from CPS that is not present in JSON V4 records.
- TWG (Lisa Olson)
  - Recent meeting discussion has focused on the CVE Services schedule and new action items.
  - Sprints are going well and testing is on-going. For problems found during testing, fixes are being planned and incorporated into the schedule.
  - No firm date yet for delivery or soft deploy, but getting closer.
  - Members of the Board who have time are encouraged to attend TWG meetings.
- AWG (Kris Britton)
  - Displayed CVE Services schedule shared at last week's TWG meeting.
    - Sprint 9 is underway to fix security issues identified by the Red Hat threat model.
    - Functional testing (client testing) is scheduled to complete this week.
    - Community penetration testing is planned to run from 7/18 through 7/29.
    - AWG will coordinate with TWG to make "fix now/fix later" decisions.
    - Participating in penetration testing is encouraged. If board members are aware of anyone who can help, it will be appreciated.

VulDB Issue

- VulDB is a CNA that has issued CVE IDs for vulnerabilities outside its scope.
- This is a topic that came up during VulDB's on-boarding, so they've known the scope rules from early on.

- The program has communicated by email twice with VulDB to notify them of the issue and identify the affected CVE IDs. There has been no response to date.
- The affected IDs/Records have been transferred to the correct CNAs, and the correct CNAs have been notified of the transfer.
- The program will reach out to VulDB to schedule a meeting to discuss scope.
- There was discussion about whether this may have happened because the vulnerabilities were low to moderate impact. Some CNAs may assign an ID in these cases. Appropriate escalation allows for the CNA-LR to potentially assign in these cases.
- Generally, escalation may be as follows: if a CNA remains unresponsive, their access to IDR is disabled. If this continues, outstanding IDs will be rejected. Finally, if still no response or correction, they'll be removed from the program.
- The program always works with CNAs to help them improve and be productive. Any removal from the program comes as a last resort after many attempts at corrective action and communications.
- Dave M. will reach out by phone to try to schedule a virtual meeting with VulDB representatives and the Secretariat (and a few members of the Board – Kent, Dave W, and maybe Lisa).
    - The desired outcome of the meeting is to get VulDB's understanding that they'll stay within their scope.
- Lisa Olson will follow up on the IDs transferred to the Microsoft CNA.

Open Discussion

- The Board was made aware of a mistake the program made with ID CVE-2022-25584. The published record included references directly to the end points. This is inconsistent with the program guidelines.
    - Program was made aware of the issue by the media attention it received.
    - A program response from the media was requested, and that has been provided.
    - The improper references have been removed from the record in both databases.
    - Program is looking into how the mistake was made, so it can be prevented in the future.
- Phil is working on JSON materials for the upcoming workshop. He has been coordinating with Kris, and will also reach out to Chandan and Dave W. when he returns from vacation next week. Chandan has much of the JSON related material and is out on leave/travel through August, so there may be some lag in responsiveness.
- The question was asked about the workshop/summit and whether it will be in-person, and what location arrangements have been made.
    - Kent's response was that the workshop and summit are different events. The workshop will be virtual and will be about introducing CVE Services 2.1 to the community via demos, guidance documentation, etc. The summit needs to wait until after the workshop, and may be an in-person event.
- Art M. shared in the meeting chat the slides (titled *The Future of CVE*) he used at the Global Security Vulnerability Summit 2022 in Austin in late June.

Review of Action Items

- 06.23.01 – Some progress has been made with the Vision Paper.

- 11.10.04 – Slides are done, Chris will send out.
- 10.26.02 – Consider adding routine feedback method to the CNA On Boarding process.
- 04.27.02 – Update status to Complete.
- 04.27.03 – Maybe use Tod's email to the journalist (04.27.02) as a starting point for the blog.

Next CVE Board Meetings

- 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)
- Wednesday, August 31, 2022, 9:00am – 11:00am (ET)
- Wednesday, September 14, 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 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)