CVE Board Meeting, August 18, 2021

Members of CVE Board in Attendance

☐Ken Armstrong, EWA-Canada, An Intertek Company
☒Tod Beardsley, Rapid7
☒Chris Coffin, The MITRE Corporation (MITRE At-Large)
☐Jessica Colvin JPMorgan Chase
☐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, McAfee Enterprise
☒Scott Lawler, LP3
☒Chris Levendis, CVE Program (CVE Board Moderator)
☒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.

Members of MITRE CVE Team in Attendance

☒Jo Bazar
☒Kris Britton
☒Christine Deal
☒Jonathan Evans

Agenda

2:00-2:05: Introductions and Roll Call

2:05-3:35: Open discussion items

3:35-3:55: Review of Action items (see attached excel file)

3:55-4:00: Wrap-up

New Actions items from today's Board Meeting

See attached Excel spreadsheet for open action items from prior meetings (CVE Board Meeting 18Aug21– Agenda and Action items)

#	Action Item	Responsible Party	Due	Status	Comments
08.18.01	Send updated ADP Pilot v10 presentation for CVE Board review and consideration; will be discussed and/or voted on at the next CVE Board meeting (September 1).	Kent L.		Not Started	Assigned on August 18, 2021

Discussion Items

- **SPWG Update – Kent Landfield**
  - Authorized Data Publisher (ADP) Pilot proposal, prepared by Art Manion and Jo Bazar, was presented to the SPWG.
    - The SPWG reviewed the revised presentation, addressed outstanding concerns, and agreed to submit to the CVE Board for approval.
- **ADP Pilot – Art Manion**
  - Art presented the ADP Pilot for CVE Board consideration.
  - The pilot objectives and goals are to help answer the following:
    - What value does an ADP bring to CVE Records?
    - What are the requirements for ADPs?
    - Who can be an ADP and how are they approved? Top-Level Root, CVE Board, etc.?
    - How are ADPs onboarded into the program, are they existing CNAs?
    - CNA buy-in, CNA authority, who can change CVE Records?
  - Why ADPs?
    - ADPs can help scale the CVE Program by distributing provision of additional content to other (approved) sources
    - ADPs can help add value/content that is not readily available or that an ADP is willing to contribute
    - ADPs enhance the CVE records value
    - ADPs will have their own container in JSON 5 which means they CAN NOT change data provided by CNAs
  - Why an ADP Pilot?
    - Test ADP concept operationally
    - Develop ADP guidelines based on some actual experience (not just discussion)
  - Pilot Overview
    - Communicate about pilot to CVE stakeholders
    - Develop and test ADP processes
    - Develop ADP guidance based on pilot experience
    - Test CVE services and formats ADP use (including CVE JSON 5 and Services 2.0)
    - Test value/use of ADP data (in this case, vulnerability response prioritization data using Stakeholder-Specific Vulnerability Categorization, SSVC)
  - Pilot Evaluation
    - At the end of the pilot:

a. 120 day pilot, 90 day evaluation
b. (write down goals/tests first, then pilot, then assess)

- Report to CVE Board (and eventually published), including
  a. Recommendations for next steps
  b. Input from CVE WGs (SPWG, QWG, possibly AWG)
  c. Input from other stakeholders including CVE consumers (vuln mgmt?), CNAs, community, etc.
  d. Analysis on the ADP pilot
     - What went right and what went wrong
     - What we learned from the pilot
  e. Did the pilot achieve goals?
     - Are ADPs adding value and enriching to the CVE records?
     - How do we know if the pilot was successful?
- Pilot Outcomes
  - Stakeholder Feedback (WG, CNA, CVE Consumers, etc.)
  - ADP Rules 1.0 draft to CVE Board
    a. Understand how ADP rules impact the CVE Assignment rules
  - ADP tools are developed during the pilot
  - Data produced will be integrated into CVE records
    a. Identify data from ADP pilot, can it be removed if desired?
  - Recommendations to CVE Board
    a. Deploy or not to deploy
    b. Enabling additional ADPs, based on ADP Rules 1.0
- The SPWG will send the updated presentation to the Board email list to allow the Board members who were unable to attend today's meeting the opportunity to review and provide feedback.
  - Final decision/vote will occur at the next CVE Board Meeting

- **OSS Foundation Meeting Update – Katie Noble**
  - Katie Noble and CVE Program attended a regularly scheduled OSS Foundation meeting on August 9 and conducted a type of "sensing session"
  - The meeting included the airing of grievances and understanding misperceptions regarding the CVE Program
  - There seemed to be a lack of understanding regarding the automation underway and the overall mission of the CVE Program
  - The next meeting (TBD) will focus on solutions and how to move forward
- **Public Reference Requirements – David Waltermire**
  - Question for the CVE Board:
    1. **Should the CVE Program continue with the requirements of a public reference for CVE Record submissions?**
       - This requirement is creating additional burden for smaller companies that do not have advisory locations.
       - Majority viewpoint of Board members in the meeting was that this is a public program, therefore the vulnerability must be disclosed publicly
       - QWG would like to get buy-in from the Board before this discussion is continued in the QWG
    2. **Is the CVE Master list the first point of a public reference?** What about when the original link to the reference breaks?

        - Trust comes from a specific vendor website, for people to use and confirm the issue exists.
    3. **What are our (CVE Program) culture and values? Not requiring a public reference would lower the bar.**
        - The Board agreed this is a policy problem, not a technology problem.
    4. **If the CVE record was populated with sufficient (would need to be defined) details, does it meet the transparency requirements?**
        - This means CVE Records would be the first point of publication, there is not legal concern per MITRE Legal.
- The Board did not reach consensus and will continue the discussion on the CVE Board list

Next CVE Board Meetings

- Wednesday, September 1, 2021 9:00am-11:00am (EDT)
- Wednesday, September 15, 2021 2:00pm-4:00pm (EDT)
- Wednesday, September 29, 2021 9:00am-11:00am (EDT)

Open Discussion Items (to be discussed at future meetings)

See attached Excel spreadsheet (CVE Board Meeting 18Aug21– Agenda and Action items)

CVE Board Recordings

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