CVE Board Meeting, December 8, 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
☐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

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

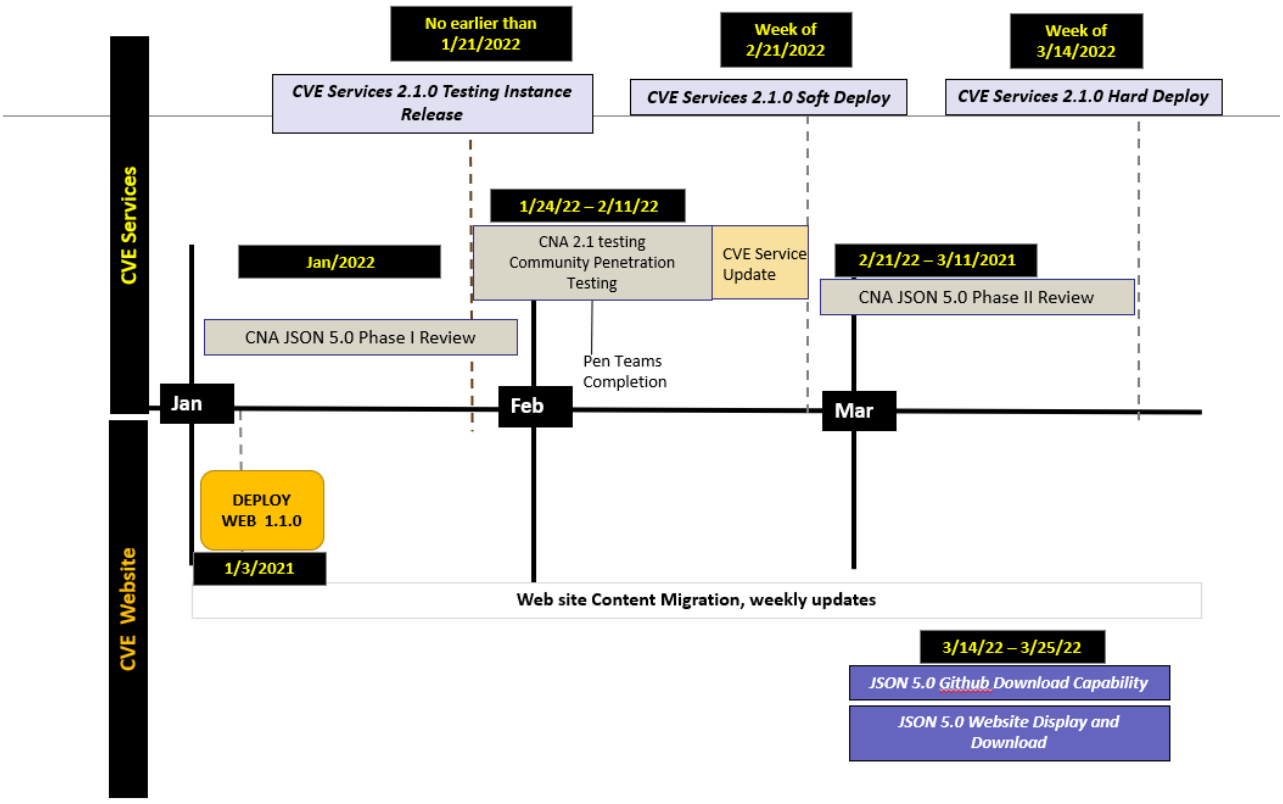
New Actions items from today's Board Meeting

See attached Excel spreadsheet for open action items from prior meetings (CVE Board Meeting 8Dec21–Agenda and Action items.xls)

	Action Item	Responsible Party	Due	Status	Comments
None					

Working Group Updates

- **Automation Working Group (AWG) Update – Kris Britton**
  - Kris provided an overview of the **AWG Year End 2021 deployment schedule** and accomplishments year to date.
  - Listed below is a summary of the 2021 Deployments and Releases:
    - CVE Services 1.1.1 was deployed June 2021; included Record Submission and Upload Service (RSUS) 1A functionality
    - CVE Service Testing/Staging Instance was deployed September 2021
    - CVE Services 2.0.0 was released for community testing September 2021;includes RSUS 1B functionality
    - New Website 1.0.0 (Beta) (cve.org) was deployed September 2021
    - CVE Service Clients were also deployed: Red Hat CLI client and Vulnogram JSON 5.0 support
  - The AWG hosted community engagements to support CVE Services rollout
    - Two CVE Services Workshops: Developer focused workshop in September 2021, and CNA focused in October 2021; both included briefs from the community about CVE Services 2.x/JSON 5.0
    - Weekly AWG meetings, open to the community; average attendance 12-16 (1/3 MITRE, 2/3 non-Mitre)
  - AWG did not accomplish everything they wanted to, including:
    - Website 1.1.0 deployment
    - Retire cve.mitre.org completely
    - Production deployment CVE Services 2.1.0, accompanied with roll-out of JSON 5.0
  - Kris reviewed the Proposed 1QT 2022 Deployment/Release Schedule (see chart below)



- No Board members objected to the schedule update

- **Quality Working Group Updates – Kris Britton on behalf of QWG**
  - Kris provided an overview of the **CNA JSON 5.0 Record Review Framework Proposal** for the Board buy in
    - The objective of the proposal is to have CNAs review their JSON 5.0 historical records for discrepancies that have been introduced as a result of the "upconvert" process.
  - Listed below is the proposed framework:
    - **Secretariat to "upconvert" to JSON 5.0** a "snapshot" of the CVE Repository and place this snapshot into GitHub for review
      - Much like the CVE List, GitHub 4.0 CVE List is published today
      - Proposed availability December 15, 2021 (this could slip based on AWG comments received December 7)
      - A snapshot review will be facilitated by the QWG in two phases
    - **QWG leading historical JSON 5.0 Record CNA review**
      - **Phase I: Focused Review**
        a. Reaching out to "key", individual CNAs to request a spot check review of their historical records
        b. CNAs selected for this effort will have access to:
           - Upconverted Snapshot on GitHub
           - Information about which CVE Records the Secretariat has record of them "owning" (i.e., a spreadsheet)

c. Proposed Timeline: January 2022

- **Phase II: General Community Review**
  a. A broader review in which the whole community is invited to review their historical CVE Records
  b. CNAs performing for this effort will have access to:
     – Upconverted snapshot on GitHub
        – x_v4-legacy-record as an additional "optional field" containing V4 source data to facilitate review
        – Inserted as part of the upconvert process
     – Information about which records the Secretariat has records of the CNA owning (i.e., a spreadsheet)
     – CVE Services 2.1.0 (in production) to review records and make corrections
- Time Frame: Post CVE Services "soft deploy" (proposed late February/early March 2022)

– Proposed Framework

- A QWG "Adjudication Group" will review the "findings" for each phase and determine whether:
  a. The finding is systemic and identifies a flaw in the "upconverter" (1st phase)
  b. The finding is not systemic (and will need to be addressed by the CNA)
- "Systemic" "upconverter" findings will result in modifications in the JSON 5.0 "upconverter"
  a. Possible schedule impact
- "Non systemic" findings will be the responsibility of the CNA to correct during the CVE Services 2.1 Soft Deployment period
  a. February/March 2022
- How we will collect feedback
  a. Groups.io email subgroup just for this purpose
     – Members are the Adjudication Group
     – CNAs send their findings to the group
- Adjudication Group
  a. Subgroup of the QWG
     – AWG/Developer membership
  b. Objective:
     – Review each finding and categorize it as "systematic" or "non-systematic"
     – Respond to each CNA noting the finding disposition (noting what they have to do next)

– JSON 5.0 "Soft Deploy" and the CNA Community Historical Record Review

- CVE Services 2.x/JSON 5.0 will undergo a "soft deploy" in the first month of service meaning:
  a. CVE Repository upconverted to JSON 5.0 – becomes the gold copy
     – As previously decided
        - JSON 4.0 records will be maintained until June 2022
          - Includes downconverter development/testing

- JSON 5.0 submission will be accepted through CVE Services
- Web Form submission still supported
- JSON 4.0 bulk download web site on GitHub still supported

- **Decision 1:**
  - CVE Board agreed with the recommendation for the CNA JSON 5.0 Record Review Framework Proposal (10 voted)
- **Decision 2:**
  - Board decided that the upconverter discussion/design feedback should happen in the QWG as opposed to the AWG.
- **Strategic Planning Working Group Update – Kent Landfield**
  - SPWG made the recommendation for CVE References ADP Pilot same time as SSVC ADP pilot at next CVE Board Meeting
    - All TLRs will be able to benefit from CVE References ADP Pilot
    - MITRE / Secretariat will modify their CVE Reference scrapping automation to use the public CVE Service ADP APIs to provide the same reference information currently being performed today
    - ADP References will be added using an ADP container that identifies the ADP
    - ADP Container will be listed as attributed to the CVE Program such as CVE Program References allowing downstream consumers of CVE data to be able to recognize this is base level information that should be included by default
    - The intent of this pilot is to test the services and to have it structured in much the same way as the SSVC pilot as to validation of outcomes and success.
    - APDs are approved by the CVE Board
  - AWG has not implemented or gathered requirements for the ADP pilot.
- **Decision 3:** CVE Board agreed with the SPWG recommendation to have the CVE References ADP Pilot run concurrently with the SSVC ADP Pilot (11 voted)
- **Outreach and Communications Working Group – Shannon Sabens/Jo Bazar**
  - **CVE Blog Posts**
    - Published Blogs
      - 200+ Organizations Now Participating as CVE Numbering Authorities (CNAs) – November 16
      - CVE Program Report for Q3 Calendar Year 2021 – November 16
    - Pending: December
      - OUR CVE STORY: "CERT@VDE"
      - Q3-21 Working Groups Progress Report Update & Recruitment
      - CVE Global Summit Autumn 2021 Summary Report
  - **"We Speak CVE" Podcast**
    - Published:
      - Podcast #10 "How Red Hat's Active Participation Helps Improve the CVE Program" - November 30
      - Shannon Sabens of CrowdStrike chats with Peter Allor, Fabio Oliveira, and Martin Prpic of Red Hat, which is a long-time CVE Numbering Authority (CNA). The benefits of actively participating as a member of the CVE community are discussed, especially in the CVE Working Groups, which allows Red Hat to directly contribute to enhancing CVE automation and quality, as well as strategic planning for future improvements.

- Podcast planning underway
  - Topic: ADP Pilot (Art Manion)
    a. Podcast recorded and publication date is planned for December 14
  - Topic: How financial services use CVEs, Jessica Colvin (JP Morgan Chase) - ON HOLD until January 2022
  - Future Podcasts:
    a. GitHub (Topics of their choice)
    b. Hacker One (Topics of their choice)
    c. Topic: CVE Myth Busters
       - Part 2: TBD
- **CVE Website Content Review**
  - A small team of OCWG members (Content Sub Working group)
  - Developing process for CVE community to provide feedback and disseminate to appropriate owners
  - Content migration strategy developed and in progress working with the TWG and Website Working Group
  - OCWG is working closely with development team to define requirements for Content Management System

- **CNA Coordination Working Group Update: Tod Beardsley**
  - No updates

Next CVE Board Meetings

- Wednesday, December 22, 2021 9:00am-11:00am (EST) - CANCELED
- Wednesday, January 5, 2022 2:00pm-4:00pm (EST)
- Wednesday, January 19, 2022 9:00am-11:00am (EST)

Open Discussion Items (to be discussed at future meetings)

See attached Excel spreadsheet (CVE Board Meeting 8Dec21– Agenda and Action items.xls)

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).