CVE Board Meeting – 21 August 2019

Tod Beardsley, Rapid7
William Cox, Synopsys, Inc.
Patrick Emsweller, Cisco Systems, Inc.
Kent Landfield, McAfee
Beverly Miller Alvarez, Lenovo Group Ltd.
Scott Moore, IBM
Lisa Olson, Microsoft
Shannon Sabens, Trend Micro
Takayuki Uchiyama, Panasonic Corporation
David Waltermire, National Institute of Standards and Technology (NIST)
Ken Williams, Broadcom Inc.

Members of MITRE CVE Team in Attendance
Jo Bazar
Chris Coffin
Christine Deal
Jonathan Evans
Chris Levendis
Lew Loren

Agenda

2:00 – 2:15: Introductions, action items from the last meeting

2:15 – 2:30: Working Groups

- *Outreach and Communications Working Group (OCWG):* Shannon Sabens
- *CNA Coordination Working Group (CNACWG)*: Tod Beardsley
- *Quality Working Group (QWG):* Chris Coffin
- *Automation Working Group (AWG)*: Lew Loren
- *Strategic Planning Working Group (SPWG):* Kent Landfield/Chris Coffin

2:30 – 2:45: Root CNA Update

- *MITRE*: Jonathan Evans
- *JPCERT*: Jonathan Evans/Chris Coffin

2:45 – 3:15: CNA Summit 2020

3:15 – 3:55: Open Discussion

3:55 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held on 24 July 2019

#	Action Item	Responsible Party	Status	Comments
1.23.1	Assemble additional operational guidance for program participation by CNAs (e.g., webinars, instructional videos).	MITRE (Evans/Sain)	In Process	MITRE assembled a list of guidance priorities and other areas of the program; the top five priorities are listed below: 1. How to submit entries to MITRE using the web form 2. CVE ID assignment rule (Counting) 3. Becoming a CNA 4. CVE Program (includes Root structure) 5. How to request the MITRE CNA populate a CVE entry 8/21 Update: Jonathan sent draft CNT1 and CNT2 to OCWG and CNACWG for review and feedback by 9/13/19.
4.17.5	Research solution for storing, archiving, and central repository for CVE Board and WG meeting minutes, recordings, as well as tracking action items.	MITRE (Lew L.)	In Process	6/12 Update: CNA SharePoint site is up (MITRE partners account is required), Handshake account is used for current meeting recordings and we are moving the archive of recordings to Amazon glacier for cold storage. 8/21 Update: Next step is to move the recordings to the Amazon glacier for cold storage.
6.26.2	Update Charter to reflect new interview process of board nominations and that CVE Board member can send nominations directly to the private board list.	MITRE (Chris C.)/Kent L.	Not Started	Assigned 6/26/2019
6.26.3	Update Charter to reflect new Board nomination interview process. When a new Board member is nominated, a 30-minute interview is conducted during the next Board call.	MITRE (Chris C.)/Kent L.	Not Started	Assigned 6/26/2019
7.24.01	Develop a strategy for handling public but low-quality vulnerabilities, especially cases where the vendor or maintainer has not acknowledged the vulnerability.	MITRE (Chris C./Jonathan E.)	Not Started	Assigned July 24, 2019

#	Action Item	Responsible Party	Status	Comments
7.24.02	Draft language clarifying CVE charter around organizational voting. (When do we merge votes based on organizational affiliation)	MITRE (Chris C.)/Kent L.	Not Started	Assigned July 24, 2019

Working Group Updates

- *Outreach and Communications Working Group (OCWG): Shannon Sabens*
  - Kickoff meeting held on August 2:
    - The group brainstormed about different ways to target CNAs. A shopping list of items was created that includes tasks to be tackled in future meetings. OCWG will meet every other Friday, alternating with the CVE Board meeting weeks.
  - OCWG meeting held on August 16:
    - The group discussed additional CNA outreach strategies, including utilizing the conferences and participating in talks to promote the program.
    - The group discussed hosting a contest that would be open to the community to create a new CVE logo. The group agreed this would be good for re-branding CVE and for action for the OCWG.
- *CNA Coordination Working Group (CNACWG): Tod Beardsley/Chris Coffin*
  - CNACWG meeting held on August 14, 2019:
    - The group discussed the rules revisions assigned to the working group and they plan to finalize the revisions in the following meeting, August 22, 2019. In addition, the group discussed how to deal with CNAs not following the CNA rules.
  - In July, the SPWG and AWG briefed the group on status updates on projects being worked in each working group.
  - CNACWG will plan the next virtual CNA summit, tentatively scheduled for mid-October. The focus will be on the proposed rules revisions from all the working groups.
- *Quality Working Group (QWG): Dave Waltermire/Chris Coffin*
  - No meeting last week. Next meeting is August 22, 2019.
- *Automation Working Group (AWG) – Lew Loren*
  - AWG meeting held on Monday August 18 and Tuesday, August 19:
    - At both meetings, Matt Bianchi gave a demo of the AWG work board, the public facing work board that will be used for the AWG. The work board will be a single landing spot for submitting future requests, bug reports, pull down tasks to contribute to the open source effort, source codes, milestones, and tags.

- On September 9, the AWG will provide a status update on the AWG projects to the SPWG; the meeting will be 2 hours.
- The Board agreed there is a communication gap that needs to be bridged between the AWG and SPWG:
  - Lew Loren will develop and create a project plan with milestones, dependences and due dates that will help address this issue.
  - As major milestones are being met, the SPWG should be briefed by the AWG. The SPWG should brief the AWG as new requirements arise and priorities changes.
  - The SPWG and the AWG should hold a joint meeting at least monthly to provide status updates.

- *Strategic Planning (SPWG) – Kent Landfield/Chris Coffin*
  - Meeting held on Monday, August 19:
    - The EOL issue was discussed and there were three options:
      1. Option 1: Current Process
      2. Option 2: Note EoL Status in the CVE Entry:
         a) Include in the description (good for the CVE consumer)
         b) EoL tag (good for filtering and metrics)
      3. Option 3: CNA-LR no longer assigns and populates for CNA EoL products
  - Kent is moving forward with a draft proposal that provides more detail and process for option 2. It will also provide more specifics on when the tag and extra information can be used and when they cannot (tag should only be used when CVE is assigned, and the affected product is EOL at the time of assignment).

CNA Updates

- *MITRE – Jonathan Evans/Jo Bazar*
  - There were 2 requests to become a CNA
    - CNA1 (Vendor)
    - CNA2 (Researcher)
  - 2 On-boarding Sessions this week.
  - 3 New CNA Announcements coming soon.
- *JPCERT - Jonathan Evans/Chris Coffin*
  - No Updates.

CNA Summit 2020

- **CNA Summit 2020 (In Person)**
  - Beverly Miller Alvarez (Lenovo) has offered to host the next CNA Summit (In Person) March 2020
  - NetApp will be hosting the FIRST-TC in Raleigh, NC
    - FIRST-TC Conference will be Wednesday, March 4 and Thursday, March 5
  - Lenovo is right around the corner from NetApp

- CNA Summit is tentatively scheduled for Monday, March 2 and Tuesday, March 3
- Beverly has reserved conference rooms to accommodate at least 100 people

Open Discussion Items

- None

Action Items from Board Meeting held on 21 August 2019

#	Action Item	Responsible Party	Status	Comments
8.21.01	Take the lead for contest open to the community to create new CVE logo.	OCWG	Not Started	Assigned on August 21, 2019
8.21.02	Send email to CVE Board about CNA Summit in March 2020.	MITRE (Jo Bazar)	Not Started	Assigned on August 21, 2019
8.21.03	Set up recurring status meeting with AWG and SPWG (Monthly).	MITRE (Lew Loren)	Not Started	Assigned on August 21, 2019

Board Decisions

- None

Future Discussion Topics

1. Communication
    a. Outreach **OCWG** for most of this section (noted otherwise).
        i. Localization – should start in the QWG for guidance, then to the AWG for implementation.
        ii. Upstream producers –
            1. CNA Recruitment
        iii. Downstream users –
        iv. Related Projects
            1. Vulnerability Description
                a. VDO
                b. CSAF
            2. Severity
                a. CVSS
            3. Product identification and management
                a. SBOM
            4. CWE
                a. hardware

    b. Metrics – **CVE Board**
        i. Community metrics (Public metrics)
        ii. CNA specific metrics
        iii. Program performance (Report card)

    c. Knowledge capture/transfer - **CVE Board**
        i. Record Working Group meetings
            1. Where to store the recordings?
        ii. Issue tracking
        iii. Storage of WG materials – SharePoint site (CVE CNA site)

2. Strategy
    a. Program Structure **SPWG**
    b. Roles, responsibilities, and requirements **SPWG**
        i. Disclosure Policies
        ii. Scope
            1. Non-vendor CNAs
                a. Add new non-vendor CNAs is on hold until the Board can come to an agreement on the requirements for this type of CNA
            2. Root CNA shopping
            3. Assigning CVE IDs to vulnerabilities in a non-CNA vendor's product
            4. CNA scope to the cooperative sub-CNAs

c. Coverage – **CVE Board**
    i. What's in, What's out
    ii. End of life
    iii. Software as a service
    iv. Hardware
        1. Define (not a wrench)
    v. Open source software
d. Goals - **CVE Board**

3. Operations
    a. Guidance
        i. Operationalizing Root CNAs - **SPWG**
            1. What is MITRE's role
            2. How to best operationalize Root CNAs
        ii. For new CNAs - **CNACWG**
            1. What is needed?
            2. What are the best formats?
            3. How to minimize one-on-one guidance
        iii. How to supply refreshers **CVE Board/CNACWG**
    b. CNA Management - **CNACWG**
        i. CNA Process – Front Door or Back Door: How should CNAs communicate with each other, and how would that information be managed?
        ii. Requirement
            1. Responsiveness
            2. Time to populate
            3. RBP start time
        iii. Scope statement best practices
        iv. Rules Violations
            1. Assignment correction processes (e.g. reject, split, merge) should account for violations
    c. Assignments – **CVE Board**
        i. Prevent duplicates
            1. How can CNA scopes help?
    d. Submissions **QWG and CVE Board, AWG handle format implementation**
        i. Formats
        ii. Information requirements
            1. Add impact
            2. Add publication data
            3. Add vulnerability type

4. Split problem type in to vuln. type, root cause, or impact
5. Don't require references

iii. Should the description match the separate metadata fields

4. CVE List - **QWG**
   a. Formats (all different formats) – **CVE Board**
      i. How can the download formats be updated or retired?
   b. CVE Tagging
      i. Helps filtering
      ii. How to identify the categories we need
      iii. Should the tagging be attached to the product or the vulnerability?
      iv. Could we leverage a product listing the CVE User Registry?
      v. Can it be automated?
      vi. EOL tagging
   c. Prose description, do we need it?