CVE Board Meeting – 4 September 2019

Tod Beardsley, Rapid7
Patrick Emsweller, Cisco Systems, Inc.
Scott Lawler, LP3
Beverly Miller Alvarez, Lenovo Group Ltd.
Scott Moore, IBM
Shannon Sabens, Trend Micro
Kathleen Trimble, U.S. Department of Homeland Security (DHS)

Members of MITRE CVE Team in Attendance
Chris Coffin
Christine Deal
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/Jo Bazar
- *JPCERT*: Jonathan Evans/Chris Coffin

2:45 – 3:00: CNA Summit 2020 – Updates

3:00 – 3:55: Open Discussion

3:55 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held on 21 August 2019

#	Action Item	Responsible Party	Status	Comments
1.23.1	Assemble additional operational guidance for program participation by	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:

#	Action Item	Responsible Party	Status	Comments
	CNAs (e.g., webinars, instructional videos).			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.)	In Process	9/4 Update: Outline drafted by Jonathan and is being reviewed by the CVE team.
7.24.02	Draft language clarifying CVE charter around organizational voting. (When do we merge votes	MITRE (Chris C.)/Kent L.	In Process	Assigned July 24, 2019

#	Action Item	Responsible Party	Status	Comments
	based on organizational affiliation)			
8.21.01	Take the lead for contest open to the community to create new CVE logo.	OCWG	In Process	9/4 Update: OCWG discussed at last meeting and is seeking additional guidance from the CVE Board.
8.21.02	Send email to CVE Board about CNA Summit in March 2020.	MITRE (Jo Bazar)	Completed	9/4 Update: Email sent on August 27; no objections with Lenovo hosting 2020 CNA summit.
8.21.03	Set up recurring status meeting with AWG and SPWG (Monthly).	MITRE (Lew Loren)	Not Started	Assigned on August 21, 2019

Working Group Updates

- *Outreach and Communications Working Group (OCWG): Shannon Sabens*
  - OCWG meeting held on August 30, 2019:
    - The group discussed CNA targets, CNAs at conferences, and outreach opportunities. Shannon drafted the CNA Press Release Template for CNA Coordinator team to review. OCWG is actively working on setting up the CVE logo contest.
  - Tod Beardsley asked Chris Coffin and Katie Trimble to participate in a Security Nations podcast.
  - CVE Logo Contest:
    - Chris Coffin provided some guidelines from the MITRE perspective: He explained that the new logo should not have any weapons or targets in the logo; needs international representations; and CVE mission, value, and purpose should be incorporated.
    - Shannon Sabens will follow up with Tod about the contest since he has previous experience with open community contests.
    - Tod suggested that we reserve the right to modify the winning logo submission. Apart from that, the process for setting up the contest should be straightforward.
- *CNA Coordination Working Group (CNACWG): Tod Beardsley/Chris Coffin*
  - CNACWG meeting held on August 28, 2019:
    - The group continued work on rules revisions around scope statement and CNAs not following the CNA rules.
    - CNACWG will plan the next virtual CNA summit, tentatively scheduled for October 15, 2019. The focus will be on the proposed rules revisions from all the working groups.
- *Quality Working Group (QWG): Dave Waltermire/Chris Coffin*

- QWG meeting held on August 22, 2019:
  - The group used this meeting to catch up on the CNA rules revisions assigned to the QWG. Chris Coffin introduced a proposed rules revision regarding required fields: Are the current fields enough, or do we need more?
  - Dave and Chris are working on proposals for the rules revisions that are due on October 1, 2019.
  - The next QWG meeting is scheduled for September 5, 2019.
- *Automation Working Group (AWG) – Lew Loren*
  - AWG meeting was cancelled on September 2, 2019, due to U.S. holiday.
  - Lew is putting together a briefing for the SPWG for the September 9, 2019 meeting.
  - Creative Common Zero license was supposed to be posted to GitHub; instead, Creative Commons variance was mistakenly posted. MITRE legal was consulted and there is not an issue with swapping out the licenses.
  - On March 2019, 270 entries got mangled in Github. The developers were able to salvage 250 of the entries; however, the remaining 20 will need to be manually fixed.
- *Strategic Planning (SPWG) – Kent Landfield/Chris Coffin*
  - SWPG meeting cancelled on August 26 and September 2.
  - Kent is working on finalizing the EOL recommendation.
  - The next meeting is scheduled for September 9, 2019.

CNA Updates

- *MITRE – Jonathan Evans/Jo Bazar*
  - We received five CNA requests since the last CVE Board meeting.
  - We conducted two on-boarding sessions this week.
  - CNA Announcements this week:
    - Two new CNA announcements this week: Bitdefender and Saleforce, Inc.
    - One CNA announcement pending.
    - There are now 102 CNAs participating in the program

- *JPCERT - Jonathan Evans/Chris Coffin*
  - No Updates.

CNA Summit 2020

- **CNA Summit 2020 (In Person)**
  - Planning is underway. Beverly was able to obtain the attendee list from the PSIRT TC and there is some overlap, which will hopefully increase the CNA Summit attendance. Beverly will keep the group updated on a regularly basis.

Open Discussion Items

- None

Action Items from Board Meeting held on 4 September 2019

#	Action Item	Responsible Party	Status	Comments
9.04.01	Review CNA Press Release Template from OCWG.	MITRE (Jo B./Jonathan E.)	Not Started	Assigned September 4, 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?