CVE Board Meeting – 2 October 2019

Tod Beardsley, Rapid7
Mark Cox, Red Hat, Inc.
William Cox, Synopsys, Inc.
Patrick Emsweller, Cisco Systems, Inc.
Kent Landfield, McAfee
Beverly Miller Alvarez, Lenovo Group Ltd.
Scott Moore, IBM
Lisa Olson, Microsoft
David Waltermire, National Institute of Standards and Technology (NIST)
Ken Williams, Broadcom Inc.

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

2:45 – 3:00: Virtual CNA Summit – Agenda - Tod Beardsley

3:00 – 3:55: Open Discussion

3:55 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held on 18 September 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)	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. 10/2 Update: Jonathan has drafted the Assignment rules script and will send to the group for review and feedback.
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. 10/2 Update: Script is being developed so the current meeting recordings can be uploaded to Amazon Glacier.
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.	In Process	10/2 Update: Kent explained a draft is in process; once completed, Chris C. will provide his input and send to the CVE Board for review and feedback. The CVE Board should expect to receive a draft in the next few weeks.
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.	In Process	10/2 Update: Kent explained a draft is in process; once completed, Chris C. will provide his input and send to the CVE Board for review and feedback. The CVE Board should expect to receive a draft in the next few weeks.

#	Action Item	Responsible Party	Status	Comments
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 based on organizational affiliation)	MITRE (Chris C.)/Kent L.	In Process	10/2 Update: Kent explained a draft is in process; once completed, Chris C. will provide his input and send to the CVE Board for review and feedback. The CVE Board should expect to receive a draft in the next few weeks.
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.
9.04.01	Review CNA Press Release Template from OCWG.	MITRE (Jo B./Jonathan E.)	In Process	10/2 Update: MITRE Corporate Communications provided feedback; OCWG is reviewing.

Working Group Updates

- *Outreach and Communications Working Group (OCWG): Shannon Sabens*
  - OCWG meeting held on September 27, 2019: The group talked about targeting companies that have CVE ID's and have not requested to be a CNA. Jonathan has put together a draft list.
    - The introduction letter has been drafted for potential new CNAs; it is almost done. Once drafted, the OCWG will send to MITRE and the group for review and feedback.
    - Shannon spoke to Tod about the CVE Logo contest and his experiences with the 99designs (https://99designs.com/). The OCWG has additional questions for the CVE Board:
      - What is the expected time frame?
      - How will we promote the contest?
      - Do we have any commitment to purchasing any of their packages?
    - OCWG meeting times will change; a meeting poll will be emailed to the group to determine a better time for everyone.
- *CNA Coordination Working Group (CNACWG): Tod Beardsley/Chris Coffin*
  - CNACWG meeting held on September 25, 2019:
    - The group finalized the draft CNA Virtual Summit agenda and sent it to the CVE Board for review and feedback.

        - At the next CNACWG meeting, we will be opening up nominations for a new chair for the CNACWG; there will an election process.
- *Quality Working Group (QWG): Dave Waltermire/Chris Coffin*
    - QWG meeting held on September 19, 2019:
        - Chris C. provided an update via email. In the last meeting, the group talked about the minimum requirements for a CVE entry and worked on finalizing their assigned rules revisions proposals.
- *Automation Working Group (AWG) – Lew Loren*
    - AWG meeting was held on September 30, 2019:
        - Lew explained the AWG will place greater emphasis on user registry, and authentication services. Developers are looking into various options: Developer #1 is looking at how this will fit with the architecture being developed in the AWG, and Developer #2 is looking at the available options with Amazon Web Services offering something for user registry and authentication, but it's unclear where their support ends and ours picks up.
        - It was pointed out that the JSON Scheme we are currently using is in draft form and needs to be finalized. Part of the finalization is adding a place for the CVSS scores; Chandan agreed to take a first cut at it for us.
    - Joint SPWG and AWG meeting held on September 25, 2019.
        - Meeting reviewed the documentation and guidance focused on user registry. The purpose was to refine the requirements so that they are actionable for the AWG, so implementation can be the focused and we can worry less about the interruption. Lew sent out draft notes but will be following up with finalized notes that include anything that may have been missed.
- *Strategic Planning (SPWG) – Kent Landfield/Chris Coffin*
    - SPWG meeting was held on September 30, 2019:
        - Most of the meeting addressed the Rules Revisions proposals, which have been submitted to the CNA Coordination team. Kent reminded the group that the Rules Revisions were due on October 1, 2019, and this was a hard deadline. Please submit your proposed rules revisions as soon as possible.

CNA Updates

- *MITRE –Jo Bazar*
    - We received two CNA requests since the last CVE Board meeting:
    - CNA1 has decided to hold off on becoming a CNA.
    - We conducted three on-boarding sessions since the last boarding meeting.
    - We have two onboarding sessions in October 2019.
    - CNA Announcements and news this week:
        - One new CNA announcements this week: HCL Software
        - There are now 103 CNAs participating in the program
        - 60 in CNA pipeline, with 35 entering the pipeline this calendar year. 7 = Q1; 11= Q2; 20= Q3 so far.
        - Three pending CNA Announcements.
- *JPCERT - Jonathan Evans/Chris Coffin*

- No updates.

Open Discussion Items

- **CNA Virtual Summit – Agenda**
  - The board reviewed the draft agenda and approved the agenda as-is. Tod will send the agenda to the CNA Discussion list.

Action Items from Board Meeting held on 2 October 2019

#	Action Item	Responsible Party	Status	Comments
10.2.19	Send CNA Virtual Agenda to CNA discussion list and attached to meeting invite.	Tod Beardsley/Jo Bazar	Completed	Sent on October 2, 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?