CVE Board Meeting – 29 May 2019

Kent Landfield, McAfee
Beverly Miller, Lenovo Group Ltd.
Scott Moore, IBM
Lisa Olson, Microsoft
Takayuki Uchiyama, Panasonic Corporation
Ken Williams, Broadcom Inc.

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

Agenda

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

2:15 – 2:30: Working Groups

- *CNA Coordination Working Group (CNACWG)* - Tod Beardsley
- *Quality Working Group (QWG):* Dave Waltermire/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* – Taki Uchiyama

2:45 – 3:55: Open Discussion – Board

3:55 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held on 15 May 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 4/3 Update: Jonathan has started assigning some of the individual modules to members of the CNA coordination team and content team. In addition, the CCWG is also reviewing and updating the existing online guidance.
2.6.9	Organize an event at Blackhat USA (August 2019) to celebrate 20 years of CVE.	MITRE (Joe S./Levendis)	In Process	5/15 Update: Approval received for the 20-year celebration at Blackhat USA, in Las Vegas. 5/29 Update: Meeting room logistics underway and being routed through MITRE approval process.
3.20.1	Document lessons learned from Microsoft automation submission process for other CNAs who want to move to GitHub automation process.	MITRE (Joe S.)	Not Started	5/29 Update: Meeting scheduled for Monday, June 3, with Microsoft security staff to discuss their experiences.
3.20.11	Review alternatives for public facing CVE Board discussion group archives.	MITRE (Joe S.)	In process	5/29 Update: Reviewing alternatives over the next week. Plans are to test functionality of top contenders over the next two weeks.
3.20.13	Write up GDPR and GitHub issue.	MITRE (Lew L./Kent L.)	In Process	5/15 Update: GDPR updates will be presented at the CNA Summit by the SPWG.
4.17.1	Assemble list of ***conferences and key meetings,*** call for Papers and due dates and add to CVE Board Agenda	MITRE (Jo B.)	In Process	Draft list sent to CVE Board on May 10. 5/15 Update: MITRE Team will add categories to each conference; community involvement, promote CVE Program, and CNA recruitment.

#	Action Item	Responsible Party	Status	Comments
	(Include 3rd vulnerability summit May 2019)			5/29 Update: Draft categories assigned; MITRE team reviewing.
4.17.3	Break out future discussion items in the following categories: Ongoing, Future, and OBE. Report back to CVE Board and add for future discussions items.	MITRE (CVE Team)	In Process	5/1 Update: MITRE CVE Team met to review the discussion items and the future discussion items will be categorized into appropriate functional areas. 5/29 Update: MITRE team meeting this week to finalize document.
4.17.5	Research solution for storing, archiving, and central repository for CVE Board and WG meeting minutes, as well as tracking action items.	MITRE (CVE Team)	In Process	5/15 Update: Jonathan sent the SharePoint site to the working groups for rules revision collaboration and for use for other working group materials. A handshake account is required to access the site.
4.17.7	Follow up with Kurt S. about the survey results; obtain for future use in QWG.	MITRE (Chris C.)	In Process	5/15 Update: Kurt sent an email on 5/13 suggesting that the survey be closed and published as there have not been any new results since 5/2.
5.1.02	Send Cloud survey to CNA List so they can provide input.	Kurt S.	In Process	5/15 Update: Waiting on survey to close on item 4.17.1.
5.15.1	Meet at CNA Summit to create the invitation list for CVE celebration	ALL	Not Started	Assigned 5/15/2019

Working Group Updates

- CNA Coordination Working Group (CNACWG): Tod Beardsley/Chris Coffin
  - No updates. The next meeting is scheduled for Wednesday, June 5, 2019; action items from CNA Summit will be addressed at this meeting.
- Quality Working Group (QWG): Dave Waltermire/Chris Coffin
  - QWG was held on Tuesday, May 28, 2019. The QWG interviewed Mark Cox, who represents Apache and OpenSSL CNAs. The most significant takeaway from the interview is that we need to better address open source CNAs in the Root CNA documentation being developed by the SPWG. The current focus of the Root CNA documentation is on commercial vendor CNAs. The balance between speed versus quality in CVE submissions was also a key point of discussion.
  - The next QWG meeting is scheduled for Thursday, June 13, 2019.
- Automation Working Group (AWG) – Lew Loren

  - No updates since last meeting. Next meeting is scheduled for Monday, June 10, 2019.
- Strategic Planning (SPWG) – Kent Landfield/Chris Coffin
  - No updates, SPWG was cancelled due to the holiday. The CNA Summit was an excellent set of conversations that will impact work the SPWG is doing.
  - Next SPWG meeting is scheduled for Monday, June 10, 2019.

CNA Updates

- MITRE – Jonathan Evans
  - No updates.
- JPCERT - Takayuki Uchiyama
  - No updates.

Open Discussion Items

- **CNA Summit Face to Face feedback**
  - Kent Landfield noted that the event was a big improvement over last year. Among Kent's observations:
    - CVE needs to focus more on professional researcher organizations and open source products.
    - The program needs to prioritize the CNA rules and ensure that the CNA community is a key player in the process.
    - The CNACWG's work to develop the Summit agenda, working with the Board and MITRE, worked very well.
  - Beverly Miller thought that the CNA summit was a great two days of material, and that the working groups have made significant progress over the last year, which helped to answer questions and issues from previous engagements.
  - Taki Uchiyama said that he enjoyed hearing the other perspectives and status updates from the working groups.
  - Chris Levendis echoed the comments of other Board members and agreed that the program needs to focus on professional researcher organizations and open source products.
  - Lisa Olson offered to host a future summit at Microsoft. She also added it was a great experience and it was nice to see more participation this year.
- **Intel CVE Entry Discussion – CVE has a lot of products and versions.**
  - Intel reached out to Kent Landfield regarding a pending CVE submission that had been flagged for more specific version information. After reviewing the submission, it became apparent that the vulnerability covered hundreds of versions. Because of the number of products and versions affected, it is not possible to add all the products and versions impacted in the CVE entry description. Intel is anxious to have this CVE ID published sooner rather than later because of the potential impacts. The Board agreed that it was acceptable to have a link in the entry for the products and versions that are impacted. The CVE team will meet with Intel to publish this submission as soon as possible.

Agenda Items for Upcoming Meetings

- Future discussion items
- Rules Revision list
- Up and coming conferences and key meetings

Action Items from Board Meeting held on 29 May 2019

- None

Board Decisions

- None

Future Discussion Topics

1. Communication
    a. Outreach
        i. Localization
        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
        i. Community metrics (Public metrics)
        ii. CNA specific metrics
        iii. Program performance (Report card)

    c. Knowledge capture/transfer
        i. Record Working Group meetings
            1. Where to store the recordings?
        ii. Issue tracking
        iii. Storage of WG materials

2. Strategy
   - a. Program Structure
   - b. Roles, responsibilities, and requirements
     - 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
     - i. What’s in, What’s out
     - ii. End of life
     - iii. Software as a service
     - iv. Hardware
       - 1. Define (not a wrench)
   - d. Goals
3. Operations
   - a. Guidance
     - i. Operationalizing Root CNAs
       - 1. What is MITRE’s role
       - 2. How to best operationalize Root CNAs
     - ii. For new CNAs
       - 1. What is needed?
       - 2. What are the best formats?
       - 3. How to minimize one-on-one guidance
     - iii. How to supply refreshers
   - b. CNA Management
     - 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

        i. Prevent duplicates
            1. How can CNA scopes help?
    d. Submissions
        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
    a. Formats (all different formats)
        i. How can the download formats be updated?
    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?