CVE Board Meeting – 12 June 2019

Andy Balinsky, Cisco Systems, Inc.
Mark Cox, Red Hat, Inc.
William Cox, Synopsys, Inc.
Beverly Miller, Lenovo Group Ltd.
Scott Moore, IBM
Lisa Olson, Microsoft
Takayuki Uchiyama, Panasonic Corporation
David Waltermire, National Institute of Standards and Technology (NIST)

Members of MITRE CVE Team in Attendance
Jo Bazar
Christine Deal
Jonathan Evans
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 – 3:00: CVENEW Twitter feed getting CNA short names

3:00 – 3:55: Open Discussion

3:55 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held on 29 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. 6/12 Update: In process. Some of the draft scripts completed for the online individual modules and the existing online guidance are also being reviewed and updated.
2.6.9	Organize an event at Blackhat USA (August 2019) to celebrate 20 years of CVE.	MITRE (Joe S./Levendis)	In Process	6/12 Update: Contract is signed with Blackhat; waiting on confirmation of event date 8/7 or 8/8 before we can proceed with approvals. Once approved by BH, we can move forward with the event planning with Excalibur. The group agreed and the majority voted for August 7th. 6/13: Approval form sent to BAH, pending approval.
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.)	OBE	5/29 Update: Meeting scheduled for Monday, June 3, with Microsoft security staff to discuss their experiences. 6/12 Update: Microsoft lessons learned. Held meeting with Microsoft; developing summary of the discussion. Since we are shifting away from GitHub, documenting GitHub is no longer needed.
3.20.11	Review alternatives for public facing CVE Board	MITRE (Joe S.)	In process	5/29 Update: Reviewing alternatives over the next week. Plans are to test

#	Action Item	Responsible Party	Status	Comments
	discussion group archives (currently Nabble).			functionality of top contenders over the next two weeks.
3.20.13	Write up GDPR and GitHub issue.	MITRE (Lew L./Kent L.)	OBE	5/15 Update: GDPR updates will be presented at the CNA Summit by the SPWG. 6/12 Update: Since we are moving away from GitHub, mark this as closed.
4.17.1	Assemble list of ***conferences and key meetings,*** call for Papers and due dates and add to CVE Board Agenda (Include 3rd vulnerability summit May 2019)	MITRE (Jo B.)	Completed	6/13/2019: Sent updated list to CVE Board on June 13th, with categories included.
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. 6/11: Future discussion items were revised in 5/29 meeting minutes, for review and comment by the CVE Board.
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. 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.
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.

#	Action Item	Responsible Party	Status	Comments
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
  - Met on Tuesday, June 4, 2019. The group discussed:
    - CVE rules revisions due 10/1/2019
    - Documentation refresh for onboarding and GitHub
    - Addressing CNACWG membership and participation
    - CVE press kit
- Quality Working Group (QWG): Dave Waltermire/Chris Coffin
  - Met on Tuesday, May 28, 2019, and Mark Cox was interviewed. Chris Coffin was not on the call to provide updates.
- Automation Working Group (AWG) – Lew Loren
  - Met on Monday, June 10, 2019. Continuing progress on the existing three services:
    - CVE ID Allocation
    - CVE User Registry
    - Credentialing, Authentication, and Authorization
  - CVE User Registry and Authorization Services will be uploaded soon.
  - The next work item is the user upload service, which is the planned replacement for GitHub. The notional plan is to set up end points so major companies like IBM and Microsoft can begin developing in-house tools. We will be adding a UI front end in the redesigned website.
  - As the other services and websites take shape, we will be demoing them in the AWG meetings as well as the other working groups for feedback.
  - The CVE Working Group meeting was cancelled this week.
- Strategic Planning (SPWG) – Kent Landfield/Chris Coffin
  - Met on Monday, June 10, 2019. Kent and Chris Coffin were not in attendance; Jonathan and Beverly provided updates for the CVE board meeting.
  - The group agreed that the Root Roles and Responsibilities prose document needs to be drafted before they can define the other roles (CNA of Last Resort, ADP, Standard and sub CNA, and Mentors).
  - The group discussed the End of Life issue; Beverly took the action to follow up with Tod about EOL problem statements. Listed below are the SPWG recommendations:

1. Assign problem statements to the CNACWG and the development of recommendations to the SPWG.
2. Send recommendations to the CNA list for review and edit.
3. Next step is to send to the CVE Board.

CNA Updates

- MITRE – Jonathan Evans
  - Organizations in on-boarding process
    - Two onboarding sessions and one refresher training since the last meeting.
    - McAfee refresher training last week
    - CNA1 completed their homework and is in the process of becoming a CNA
  - Removals
    - Riverbed
  - Other News
    - CNA team will be at the FIRST conference in Edinburgh June 16 - 21
  -
- JPCERT - Takayuki Uchiyama
  - No updates.

Open Discussion Items

- **CVENEW Twitter feed getting CNA short names**
  - There is a desire to provide attribution to new, populated CVE entries, that will identify which CNA submitted the CVE ID. Due to Twitter character limitations, condensed CNA names are required. The CVE team maintains a list of short names for CVE metrics; this list will be sent to the CNA email list for review and input.
- **CNA Summit 2020 (Face-to-Face)**
  - Beverly informed the group that NetApp is hosting a PSIRT-TC meeting in early March 2020 in Raleigh, NC. This would be a good opportunity to have the CNA Summit 2020.
  - Beverly will also investigate the possibility of Lenovo hosting the next CNA Summit if NetApp is unable to provide a venue.
- **CVE Marketing Working Group (CMWG)**
  - Several CNAs have expressed interest in participating in the CMWG. Jo Bazar has the action to draft up CMWG goals and objectives and send to CNA list for volunteers and participation. The following CNAs expressed interest: Beverly Miller (Lenovo), Andrea Taco (Schneider Electric), and Shannon Sabens (ZDI/Trend Micro).
  - Once the goals and objectives are finalized, the CVE Board can determine if the CMWG should be a stand-alone WG or be incorporated into the CNACWG.
- Andy Balinsky (Cisco) is retiring at the end of July and will be nominating a replacement to the CVE Board soon. Sincere thanks to Andy for his years of service and contribution to the CVE Program as a founding member of the CVE Board.

Agenda Items for Upcoming Meetings

- Future discussion items
- Up and coming conferences and key meetings

Action Items from Board Meeting held on 12 June 2019

#	Action Item	Responsible Party	Status	Comments
6.12.1	Send short names for CNA to review and provide input.	CNA Coordinators	Not Started	Assigned June 12, 2019.
6.12.2	Finalize "Trifold" or "Flyer" before CVE 20-year Milestone event in Las Vegas, on August 7th.	CVE Board (select) /MITRE	In Process	6.12 Update: Draft flyer sent to Beverly M., Kent L., Tod B., Shannon S., Andrea T. and Taki U. for review and feedback with a due date of June 28, 2019.
6.12.3	Develop Objectives/Goals for Marketing WG, send to CVE Board for review and feedback. Next step is to send to CNA List for CMWG volunteers and participation.	MITRE (Jo Bazar)	In Process	Assigned June 12, 2019.

Board Decisions

- The group agreed based on the poll results that August 7, 2019, will be the date of CVE 20-Year Milestone Event.

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?