CVE Board Meeting – 6 February 2019

Board Members in Attendance

Andy Balinsky, Cisco Systems, Inc.
Kent Landfield, McAfee
Pascal Meunier, CERIAS/Purdue University
Beverly Miller, Lenovo Group Ltd.
Scott Moore, IBM
Lisa Olson, Microsoft
Kurt Seifried, Cloud Security Alliance
Takayuki Uchiyama, Panasonic Corporation
David Waltermire, National Institute of Standards and Technology (NIST)

Members of MITRE CVE Team in Attendance

Jo Bazar
Chris Coffin
Christine Deal
Jonathan Evans
Chris Levendis
Lew Loren
Joe Sain

Other Attendees

Chris Johnson (NIST)

Agenda

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

2:15 – 2:30: Working Groups

- *Strategic Planning (SPWG)* – Kent Landfield/Chris Coffin
- *Automation (AWG)* – Chris Coffin
- *Cloud Security Alliance (CSAWG)* – Kurt Seifried
- *Quality Working Group (QWG):* Dave Waltermire/Chris Coffin
- *CNA Coordination Working Group (CCWG)*: Tod Beardsley/Chris Coffin

2:30 – 2:45: CNA Update

- *DWF* – Kurt Seifried
- *MITRE* – Jonathan Evans
- *JPCERT* – Taki Uchiyama

2:45 – 3:15: CVE Quarter 4 Report Card Slide Deck Review (Jonathan Evans**)**

3:15 – 3:45: CNA Virtual and Face-to-Face Summits: Board Suggestions for Topics and Discussions (Chris Coffin**)**

3:45 – 3:55: Open Discussion – Board

3:55 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held on 23 January 2019

#	Action Item	Responsible Party	Status	Comments
1	Assemble additional operational guidance for program participation by CNAs (e.g., webinars)	MITRE (Evans/Sain)	In Process	MITRE assembled a list of guidance priorities for this and other areas of the program.
2	Contact Booz Allen Hamilton (BAH) to determine the reasons for its inactivity as a CNA. They have not submitted any new content since becoming a CNA.	MITRE (Evans)	In Process	MITRE sent an email to Booz on February 6, 2019. Follow up email will be sent on February 20, 2019, if no response is received, consistent with the MITRE CNA's CNA inactivity policy.
3	Determine next steps for the DWF Root CNA.	MITRE/DWF/ CVE Board	In Process	Meeting was conducted on February 7, 2019. Conclusions: DWF is no longer sustainable and will stand down. MITRE will draft a community communication informing them of the change. MITRE will pick up DWF content production responsibilities while concurrently working with the Board to pursue alternatives.
4	Send latest version of the Root CNA Roles and Responsibilities document to the SPWG.	MITRE (Coffin)	Done	Sent to SPWG list on January 23, 2019. SPWG review is ongoing. The slides were used as-is in a discussion with JP-CERT and were effective is communicating Root CNA requirements. This validates the requirements at a level of minimum effectiveness, with additional revisions likely required.

5	Work with Microsoft on starting the automated submission process (similar to IBM's) and document process.	MITRE (Evans/Sain/ Coffin)	In Process	Microsoft to begin GitHub-based CVE submissions Tuesday, February 12, 2019.
6	Send an email to the Board list to initiate the CNA Rules revision process.	MITRE (Sain/Evans)	In Process	MITRE assembled a list of potential rules revisions and will perform internal review before sending to the Board. – Discussion of these items will also be targeted for the CNA Virtual Summit. – MITRE will draft CNA Rules regarding EOL Scoping issue and Note Field in JSON. – MITRE will draft clarifications to CNA rules related to RBPs and send to the Board for review. Target completion February 28, 2019.
7	Contact GitHub to determine its interest in becoming a CNA.	Microsoft (Lisa Olson)	In Process	Lisa is working on this and updates the Board on progress.

Working Group Updates

- Strategic Planning (SPWG) – Kent Landfield/Chris Coffin
  Reviewed the Root CVE Numbering Authority (CNA) Roles and Responsibilities Overview presentation. The group was able to get through half the presentation and will complete the review in the next meeting.

- Automation (AWG) – Chris Coffin
  CVE ID Allocation: Schmitty is making progress developing and documenting the technical requirements for the CVE ID Allocation service. Recommendations for the ID Allocation service will be presented at the next AWG meeting.
  - Beverly Miller has a volunteer for the CVE Entry Submission and Upload service development effort.
  - CVE User Registry: Kurt explained that there has been little participation for this effort and the project needs more participants to move the project forward. Lisa Olson recommended that Schmitty would be a good addition to the project. Lew Loren from MITRE will reach out to Schmitty to explore the idea of splitting the work.
- Cloud Security Alliance (CSAWG) – Kurt Seifried
  No updates; CSA survey is delayed until after the RSA Conference.

- Quality Working Group (QWG): Dave Waltermire/Chris Coffin
  Kick off meeting was conducted on February 7th at 2pm – 3pm EST. Initial focus is on clarifying the CVE Program's use cases, which underpin everything the program does.

- CNA Coordination Working Group (CCWG): Tod Beardsley/Chris Coffin
  Tod sent a doodle poll for kickoff meeting dates to the CCWG list, the kickoff meeting is scheduled for February 13, 2019.

CNA Updates

- DWF – Kurt Seifried
  - Jenkins is working out well as a sub-CNA.
  - The DWF backlog is almost cleared.

- MITRE – Jonathan Evans
  - Johnson Controls: Final onboarding meetings with Johnson Controls were successfully conducted. they should be announced as a CNA this week.
  - Apple: Submitted the majority of its RBPs; some formatting issues exist, and MITRE will work with Apple to get the issues resolved by the end of this week. Post Board Meeting: Lessons learned from the experience with Apple will be incorporated into the CNA submission guidance, which was unclear to Apple.
  - MITRE is developing a Root CVE Numbering Authority (CNA) Roles and Responsibilities Overview presentation to help Root CNAs better understand their roles and responsibilities.

- JPCERT
  - JPCERT will retain its Root CNA status and will document its process for managing and interacting with CNAs.

Special Topics

- Year-End and Quarterly Program Review & CNA Report (Jonathan Evans)
  - The Board reviewed the CVE Annual Summary, which provided the conclusions based on Year over Year (YoY) trends.

- CNA Virtual and Face-to-Face Summits: Board Suggestions for Topics and Discussions (Chris Coffin)
  - MITRE (Jonathan) will send the Virtual summit agenda items for review and feedback.

Open Discussion Items

- None

Action Items from Board Meeting held on 6 February 2019

#	Action Item	Responsible Party	Status	Comments
1	Document new Inactive CNA Policy; post publicly (share with DWF) and include in the new CNA rules and CNA onboarding process. Find a central location to store these types of policy changes.	MITRE (Levendis/Evans)	Assigned on 2/6/19	
2	Follow up with Microsoft on Monday, February 11, regarding how to proceed with automation of CVE submissions.	MITRE (Sain/Coffin)	Done	Microsoft will begin CVE submissions via GitHub on Tuesday, February 12, 2019.
3	Send CVE open source licensing options to the CVE Board	MITRE (Loren)	Done	Sent on February 8, 2019
4	Ask Tod Beardsley to send CCWG doodle poll to CNA list.	MITRE (Coffin)	Done	Sent on February 8, 2019. Meeting will be held on February 13, 2019.
5	Send attendees and status for Infrastructure Meetings to CVE Board list.	MITRE (Bazar)	Done	Sent on February 8, 2019
6	Lew Loren from MITRE will contact Schmitty to explore the idea of splitting the work for CVE User Registry.	MITRE (Loren)	Assigned 2/6/19	
7	Send the CNA Virtual summit agenda items to the Board list for review and feedback.	MITRE (Evans)	Done	Sent on February 11, 2019. Feedback due by February 20th. Agenda will be finalized no later than February 23, 2019.
8	Coordinate a get together at RSA Conference with CVE Board members.	MITRE (Sain/Board)	Assigned 2/6/19	
9	Organize an event at Blackhat USA (August 2019) to celebrate 20 years of CVE.	MITRE (Evans/Sain/Bazar)	Assigned 2/6/19	

Board Decisions

- None

Future Discussion Topics

1) How can the program better communicate its future vision for the evolution and sustainability of the CVE program? How can CVE better market the CVE program and communicate the changes that are being implemented?

2) How can better status and metrics be provided to community stakeholders?
3) CNA Process – Front Door or Back Door: How should CNAs communicate with each other, and how would that information be managed?
    a) Set up an excel spreadsheet to share contact info amongst the CNAs
4) CNA Scope Issues
    a) The Board discussed that CNA documentation around roles and responsibilities are needed. Current documentation is not clear, CNAs assign and populate CVEs within their scope. Scope may or may not cover CVEs for their customers.
    b) CNA Rules - The rules state CNAs must be responsive but do not provide a specific time frame. The rules state if a CNA plans to assign a CVE for a vulnerability in another vendor's product, the assigning CNA should contact the vendor and give them the option to make the assignment. This must be clarified in the rule's revision process.
    c) Root CNAs - A given Root has a scope. A portion of the scope gets delegated to a CNA (i.e., product or area of research). If a portion of the scope is not delegated to a CNA, that scope stays with the Root. It is the Root's responsibility to assign and populate as the CNA of last resort.
    d) Action Item – CNA Rules must be updated to reflect this new approach.
5) Eliminate duplicate CVEs discussion
    a) The Board discussed that specifying CNA scope will help eliminate duplicate CVE assignments. Art explained that having open communication with other CNAs when making CVE assignments is critical; keeping this communication at the CNA level (not at Root/Primary level) will help prevent duplication.
        i) Recommendation 1: Process recommendation needs to be added to CNA guidance.
        ii) Recommendation 2: CNA rules must be updated to minimize duplicate assignments.
    b) Jonathan Evans explained that duplication of CVE assignments occurs the most with DWF.
6) Researcher CNAs
    a) The Board discussed researcher CNAs that have ambiguous scopes. These CNAs have issued thousands of CVEs.
        i) Recommendation 1: Avoid adding any new researcher CNAs until there are specific guidelines for what qualifies as a researcher CNA. This includes defined scope rules yet to be determined.
        ii) Recommendation 2: Make the scope naturally programmatic for researcher CNAs.
        iii) Recommendation 3: Change the process for researcher CNAs. Who is responsible for coordinating the assignment of the IDs? Who issues the CVE ID and who populates the information? There should be an easier way for companies to request a CVE ID.
        iv) Recommendation 4: Better define roles and responsibilities for researcher CNAs.
        v) Recommendation 5: Explore the possibility of researchers participating in the CNA program without becoming CNAs.

vi) Recommendation 6: Need a testing/certification program for CNAs to make sure they can adequately perform their role, especially researchers.

b) The Board agreed to explore better solutions regarding the researcher CNA ambiguous scope issue.

7) Operationalize Root CNAs effectively
   a) Further discussion is needed regarding how to operationalize Root CNAs more effectively.
   b) Additional discussion regarding MITRE's role in operationalizing roots is needed.
8) Product Type Tagging/Categorization
   a) As the production numbers for CVEs go up, there will be an increasing need to view a subset of the overall CVE master list
   b) Define a list of common product areas/domains to be used for categorizing CVE entries (e.g.., Medical devices, automotive, industrial, etc.)
   c) The tags/categories should be attached to the products and not to the CVE entries directly.
   d) Product listings in CVE User Registry would be a potential location.
   e) Can it be automated?
9) Future of CVSS
   a) Assigning multiple CVSS to a single CVE.
   b) Hill discussions around CVSS.