CVE Board Meeting – 3 April 2019

Board Members in Attendance
Andy Balinsky, Cisco Systems, Inc.
Tod Beardsley, Rapid7
William Cox, Synopsys, Inc.
Kent Landfield, McAfee
Scott Moore, IBM
Lisa Olson, Microsoft
Kurt Seifried, Cloud Security Alliance
David Waltermire, National Institute of Standards and Technology (NIST)

Members of MITRE CVE Team in Attendance
Chris Coffin
Christine Deal
Chris Levendis
Lew Loren
Joe Sain
Anthony Singleton

Agenda

2:00 – 2:15: Introductions, action items from the last meeting (listed in the table below)

- Welcome Tod Beardsley as the CNA Liaison Board Representative

2:15 – 2:30: Working Groups

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

2:30 – 2:45: Root CNA Update

- *MITRE* – Jonathan Evans
- *JPCERT* – Taki Uchiyama

2:45 – 3:00: CNA RBPs – How many or what percentage should be allowed? – Chris Levendis

3:00 – 3:55: Open Discussion – Board

3:55 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held on 20 March 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.
1.23.2	Contact inactive CNA1 to determine the reasons for inactivity.	MITRE (Evans)	In Process	MITRE sent an email to CNA1 on February 6, 2019. Follow up email will be sent on February 20, 2019; if no response is received, CNA1 will be removed from the CNA program, consistent with the MITRE CNA Policies and Procedures (P&P) 1, "MITRE CNA Policy and Procedure for Inactive CNAs." *3/20 Update:* Response received from CNA1 on March 18th; still awaiting disclosure policy and advisory location. MITRE will respond to CNA1 again that a disclosure policy, advisory location, and submission of CVE IDs are requirements for participating in the CNA program. MITRE will request that CNA1 provide a disclosure policy and advisory location by April 8th, and if no response is received, CNA1 will be removed from the CNA Program on April 9, 2019. 4/3 Update: Still awaiting disclosure policy and advisory location. The CNA Coordination team met with CNA1 on 3/21 to further discuss these requirements, CNA1 understands what is required. CNA1 explained the disclosure policy is hung up in their legal department.
1.23.3	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

#	Action Item	Responsible Party	Status	Comments
				of the change. MITRE will pick up DWF content production responsibilities while concurrently working with the Board to pursue alternatives. 3/20 Update: Officially announced on March 7, 2019, via CVE Announcement, Twitter, and LinkedIn. Meeting with the DWF sub-CNAs the week of March 25 to ensure they understand CNA requirements. 4/3 Update: MITRE Root CNA met with DWF CNAs on 3/28; they now report to the Program Root CNA. The CNA Coordination team is meeting individually with the CNAs to go through some of the program guidance and counting/abstraction rules to verify that they understand it. Some of those meetings have already occurred and some will occur next week. Separate from the CNAs, the Program Root CNA has acquired 350 open general public DWF ID requests. It will take 2-3 weeks to work through this backlog.
1.23.5	Work with Microsoft on starting the automated submission process.	MITRE (Evans/Sain/Coffin)	In Process	Microsoft to begin GitHub-based CVE submissions Tuesday, February 12, 2019. 3/20 Update: The March data went through successfully March 20, 2019. The formatting of the data using the JSON format takes more iterations than expected (per Lisa Olson). Joe confirmed the test data was successful. 4/3 Update: Due to the complexity of Microsoft's submissions, it is taking 2 or 3 weeks to get their pull requests through. They are learning a lot and making progress.
1.23.6	Send email to the Board list to initiate the CNA Rules revision process.	MITRE (Sain/Evans)	Complete	MITRE assembled a list of potential rules revisions and will perform internal review before sending to the Board. • MITRE will draft proposed clarifications to CNA rules related to RBPs and send to the Board for review. Target completion February 28, 2019. • MITRE will draft proposed CNA Rules regarding EOL Scoping issue and Note Field in JSON. Target completion March 20, 2019. Update: Jonathan Evans sent message to Board on March 21, 2019. 4/3 Update: The CVE Board agreed to

#	Action Item	Responsible Party	Status	Comments
				review and provide feedback by the next Board meeting on 4/7.
1.23.7	Contact GitHub to determine its interest in becoming a CNA.	Microsoft (Lisa Olson)	In Process	Lisa is working on this and will update the Board on progress. 4/3 Update: Lisa is drafting an email to GitHub. Jonathan Evans reviewed the email and Lisa is nearing completion.
2.6.9	Organize an event at Blackhat USA (August 2019) to celebrate 20 years of CVE.	MITRE (Joe S./Levendis)	Not Started	Discuss with the CVE Board about event ideas for celebrating 20 years at CVE. 4/3 Update: Nothing has been started yet; Chris L. will check with MITRE to see if he can come up with anything. Board members indicated he feels like they could do some fund raising.
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	4/3 Update: Will begin documentation after next dry run (4/9).
3.20.3	Work with Schmitty to reschedule AWG meeting using Skype instead of Microsoft Team Meeting.	MITRE (Lew L.)	In process	4/3 Update: Lew L. sent an email to Schmitty and is waiting to hear back. Lew will make sure it is on the calendar by the end of the week. Next AWG meeting is 4/9.
3.20.5	Send comprehensive list of the Working Groups and Leads to the CVE Board (Send to private CVE board if contact information is provided). Include the CNA Handshake Calendar that includes the meeting times and conference information for the Working Groups.	MITRE (Jo B.)	In process	4/3 Update: The list of working groups and leads will be sent to the Board no later than 4/10.
3.20.6	Record WG meetings moving forward so attendees that cannot attend can listen to the meeting recordings.	MITRE/WG Chair	Not Started	4/3 Update: Joe S. noted the plan is to find a location for all recordings to be available for a limited amount of time and then we will keep a copy in cold storage, possibly Amazon Glacier (will look in to other options; Kurt suggested S3 bucket). Recordings will be posted for 4 weeks and then archived.
3.20.7	Submit paper for Blackhat USA, call for papers due April 8, 2019.	Kent L/ Art M./MITRE	Not Started	Due April 8, 2019

#	Action Item	Responsible Party	Status	Comments
3.20.8	Discuss how we can better handle the international community (English requirements of Guidance, Documentation, CVE IDs)	CVE Board	Not Started	4/3 Update: The group discussed various options and agreed to take this offline and discuss further in the SPWG Meetings.
3.20.9	Send a list of the domain names to the internal CVE Board list for review.	MITRE (Jo B.)	Complete	4/3 Update: Jo B. sent list on 4/1/19 with the 19 domain names purchased by MITRE. MITRE is in the process of purchasing 19 additional domain names and the newly identified domains (cve-ids.com, cve-ids.org, cve-ids.net).
3.20.10	Check Handshake to confirm availability of historical recordings of Board meetings.	Kent L.	Complete	4/3 Update: Kent L. confirmed, action complete.
3.20.11	Review alternatives for public facing CVE Board discussion group archives.	MITRE (Joe S.)	In process	4/3 Update: Joe S. is just getting started on this and will provide an update before next meeting on 4/17.
3.20.12	Provide feedback/comment on the Rules Revision email (sent on March 21, 2019 at 1:51pm by Jonathan E).	CVE Board	Not Started	4/3 Update: CVE Board members will send their feedback before the next Board meeting on 4/17.
3.20.13	Write up GDPR and GitHub issue.	MITRE (Lew L./Kent L.)	In process	4/3 Update: Lew L. sent draft to Kent; Kent is reviewing what Lew provided, and will provide comments and edits. Kent will add to the write up that explains the move (away from GitHub).

Working Group Updates

- Strategic Planning (SPWG) – Kent Landfield
  - SPWG Meeting was held on April 2, 2019. The group continued through Roles and Responsibilities slides and made some changes; new version was sent to the SPWG group.
  - The group has an action to review the updated version of the deck to make sure that the presentation/document outline flows well and to ensure that the deck is correctly organized. The SPGW will finalize the slide deck at the next meeting; MITRE will then finalize the prose.
  - The deck will be the foundational document on roles and responsibilities for Root CNAs going forward. We also need to figure out the requirements of Root CNAs so that we can recruit future Root CNAs.

- Chris L. added that the group realized a slide needed to be added that details *ongoing* training for Root CNAs, and thanked Kent for pointing this out in the SPWG meeting.

- Automation Working Group (AWG) – Lew Loren
  - AWG Meeting was held on April 2, 2019. MITRE developers provided the AWG with a quick overview of the progress made to date—the ID Allocation service code has been uploaded to the GitHub site owned and operated by the AWG (and possibly the Authentication and Authorization codes but Lew has not yet verified).
  - By the end of the week, Lew will re-establish Schmitty's bi-weekly meetings with a Skype dial-in rather than using MS Teams.
- Cloud Security Alliance Working Group (CSAWG) – Kurt Seifried
  - Based on lack of CSP commitment to this issue (15 survey replies in 2 weeks), we may want to put CVEs for Cloud issue in hibernation for a while.
  - The group had a lengthy discussion about assigning CVEs for Cloud issues and decided to continue monitoring interest.
  - Chris L. concluded the discussion with the following recommendations:
    - Assign this issue to the QWG. The QWG will discuss a taxonomy for categorizing cloud and other high-level types of affected products.
    - Revise the rules (INC3/INC5): Revising the rules will enable vendor CNAs to assign for cloud vulnerabilities without deviating from the rules. Assign the AWG and QWG to work through this issue and determine what the language of the change should be.
      - Kent added that changing the rules and adding the tagging mechanism must be done at the same time for this to work.
    - The group agreed with no objections to bring this back up in appropriate working groups and to discuss implementation.
- Quality Working Group (QWG): Dave Waltermire/Chris Coffin
  - Another meeting has not been set up yet; will set up the next meeting for the week of the April 8th.
  - Dave suggested meeting with Chris C. and Kent L. after today's board meeting to sketch out an agenda for the next meeting.
- CNA Coordination Working Group (CCWG): Tod Beardsley
  - The CCWG is setting the agenda for the May CNA Summit, (held in Mclean, VA on May 22-23). A survey was sent (to CNAs list and CVE Board members) about prioritizing the agenda items. The registration form for the May CNA summit was also sent to the CNA email list.
  - The CCWG meets every other Wednesday, the next meeting is scheduled for April 10th at 2:00pm EST.
  - We have four or five top contributors to the meetings; 12-18 callers.
  - We will insert a sentence in the charter that reminds people that the W in WG stands for Working (not watching); he will boot lurkers.
  - Chris L. asked the group to provide feedback on how CNA guidance or policies can improve, this feedback will be enormously valuable.

CNA Updates

- MITRE – Jonathan Evans
  - Not on the call.
- JPCERT - Takayuki Uchiyama
  - Not on the call.

Special Topics: CNA RBPs – How many or what percentage should be allowed? (Chris Levendis)

- Topic was introduced as part of the CCWG discussion. The SPWG will determine what an appropriate number or percentage would be for RBPs. Once complete, this proposal will be shared with the Board.

Open Discussion Items

- None

Action Items from Board Meeting held on 3 April 2019

#	Action Item	Responsible Party	Status	Comments
4.3.1	Purchase additional 16 domain names.	Chris C.	Not Started	Assigned April 3, 2019.

Board Decisions

- N/A

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.