CVE Board Meeting – 17 April 2019

Board Members in Attendance

Andy Balinsky, Cisco Systems, Inc.
Tod Beardsley, Rapid7
Kent Landfield, McAfee
Pascal Meunier, CERIAS/Purdue University
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
Chris Coffin
Christine Deal
Jonathan Evans
Chris Levendis
Lew Loren
Joe Sain
Anthony Singleton

Agenda

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

2:15 – 2:30: Working Groups

- *CNA Coordination Working Group (CCWG)*: Tod Beardsley
- *Quality Working Group (QWG)*: Dave Waltermire/Chris Coffin
- *Cloud Security Alliance (CSA)*
- *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 3 April 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)	Completed	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. 4/17 Update: CNA1 removed on 4/9/2019.
1.23.3	Determine next steps for the DWF Root CNA.	MITRE/DWF/CVE Board	Completed	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

#	Action Item	Responsible Party	Status	Comments
				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. 4/17 Update: DWF CNAs have been integrated and given new blocks of CVE IDs.
1.23.5	Work with Microsoft on starting the automated submission process.	MITRE (Evans/Sain/Coffin)	Completed	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. 4/17 Update: April's patch Tuesday was processed successfully.
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.

#	Action Item	Responsible Party	Status	Comments
				4/17 Update: Lisa met with GitHub; they are ready to go. MITRE will reach out to GitHub to initiate the onboarding process.
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). 4/17 Update: Will coordinate with Microsoft and the MITRE GitHub team.
3.20.3	Work with Schmitty to reschedule AWG meeting using Skype instead of Microsoft Team Meeting.	MITRE (Lew L.)	Completed	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. 4/17 Update: Meeting scheduled; next meeting is April 23, 2019, at 1:00 p.m. EDT.
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.)	Completed	4/3 Update: The list of working groups and leads will be sent to the Board no later than 4/10. Update: CVE Working Group List sent to CVE Private Board list on 4/10/2019.
3.20.6	Record WG meetings moving forward so attendees that cannot attend can listen to the meeting recordings.	MITRE/WG Chair	Completed	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. 4/17 Update: Use Amazon Glacier to store recordings after 4 weeks.
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.

#	Action Item	Responsible Party	Status	Comments
				4/17 Update: Gathering information on alternative hosting platforms. Plan is to begin transitioning to a new platform mid-May.
3.20.12	Provide feedback/comment on the Rules Revision process email (sent on March 21, 2019 at 1:51 p.m. by Jonathan E).	CVE Board	In Process	4/17 Update: Kent provided his feedback on 4/4.
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). 4/17 Update: Kent will be providing feedback and possibly a rewrite.
4.3.1	Purchase additional 16 domain names.	Chris C.	Completed	Domains were purchased for 1 year.

Working Group Updates

- CNA Coordination Working Group (CNACWG): Tod Beardsley/Chris Coffin
  - CNACWG meeting was held on Wednesday, April 10. The group developed a preliminary agenda for the CNA Summit on May 22 and 23that includes identified facilitators and discussion topics. The meeting will be conducted in discussion format, with facilitators presenting a few slides for each discussion item. The draft agenda was sent to the CVE Board on April 17, 2019, for review and comment.
  - To date, a total of 38 attendees have registered. May 3 is the cutoff for registration; after that time, we will not be able to accommodate additional in-person attendees.
  - We have a draft charter for the CCWG, which will be finalized in the next meeting.
- Quality Working Group (QWG): Dave Waltermire/Chris Coffin
  - QWG meeting is scheduled for April 18, 2019, at 1:00 p.m. EDT. QWG chairs and select CVE Board members met separately in preparation for the next QWG meeting:
    - Interview target list was identified and will be introduced at the April 18 meeting.
    - Rules of the road for interviews was created and will be introduced at the April 18 meeting.
    - CVE Tagging/Categorization will be discussed:
      - Related to the CVEs for SaaS vulnerabilities topic

  - Involves using high level tagging for CVE entries (e.g., SaaS, Mobile, Medical, etc.)
  - A proposed list of initial tags has been identified and will be introduced to the group at the April 18 meeting.
- Cloud Security Alliance Working Group (CSAWG)
  - CSAWG Chair Kurt Seifried was not in attendance, but provided the following update;
    - For CVE for cloud services, the survey is out, with just over 20 replies received. Mari wants to keep the survey active until the CSA Federal Summit in May. Kurt is inclined to put the CVE for cloud services into hibernation since there does not seem to be strong support or demand from the CVE Board, CSPs, or the consumers.
- Automation Working Group (AWG) – Lew Loren
  - The next CVE Workflow meetings have been scheduled; the next meeting is April 23 at 1:00 p.m. EDT. Moving forward, the meetings will be hosted using Skype instead of Microsoft Teams.
  - ID Allocation Service code has been uploaded to GitHub and shared with the AWG. The code is a wireframe module, with some functionality like generating the IDs stubbed out. The idea is to get the basic workflow in place, so the community can review and provide feedback.
  - Requirements gathering for User Registry and Authentication is in progress. Documentation from Infrastructure and Architecture Definition Meeting (held Feb. 26 and 27) is being used for the basis of the requirements.
  - The ID Allocation Services development is on hold until more progress is made on the User Registry and Authentication efforts.
- Strategic Planning (SPWG) – Kent Landfield/Chris Coffin
  - SPWG met on April 15 and continued to work on Root CNA Roles and Responsibilities Overview presentation. The group reorganized the deck to improve the flow, identified gaps, and added content.
  - They discussed the delivery format of the presentation once completed. This presentation is to be used as a starting point to help potential Root CNAs to understand their roles and responsibilities. The presentation begins with high-level bullet points and then drills into the details.
  - The group agreed that, in addition to the presentation, a more detailed document will also be needed for potential Root CNAs, so they have a deeper understanding of their roles and responsibilities. Possible formats include a Word document, webpage, etc.
    - Kent explained there is a tool that NIST and others are using to assist with uploading documents to a webpage automatically. We are still discussing different formatting options.
    - Document sections and who is documenting the more detailed parts, will be discussed in the next SPWG meeting on April 29.

CNA Updates

- MITRE – Jonathan Evans

- Bosch is close to becoming a CNA. They have almost completed the onboarding process; homework assignment has been submitted and is being reviewed for accuracy.
- Tigera and ESRI are now in the onboarding process.
- Onboarding session scheduled with Floragunn GmbH on Friday, April 19, 2019.
- DWF CNAs are now transitioned under MITRE.
- Booz-Allen Hamilton has been removed from CNA Program.

- JPCERT - Takayuki Uchiyama
  - No Updates.

Open Discussion Items

- Rules Revision process:
  - The group reviewed the CNA Rules revision email sent to the CVE Board on March 21, 2019, at 1:51 p.m.
  - The group agreed on the following process:
    - The CVE Board will be responsible for:
      1) Designating which parts of the CNA Rules each working group will manage;
      2) Prioritizing the current proposed changes; and
      3) Setting a due date for the proposed rules revisions.
    - Working groups will be responsible for:
      1) Providing a list of proposed changes;
      2) Providing reasoning behind the proposed changes; and
      3) Updating CNA Rules document with proposed changes.
    - If necessary, the working groups can consult with the Board or with other working groups on their recommended changes.
    - Once the working groups have completed their revisions:
      1) MITRE consolidates rules revisions and sends to CVE Board and CNAs for comment;
      2) MITRE consolidates comments from CNAs and CVE Board into rules revision document and sends to the CVE Board for final comment; and
      3) MITRE will incorporate the comments and produce a final draft. The Board will then vote to approve the new Rules document.
  - Next steps are to prioritize the rules revision list. Jonathan will send a survey to the CVE Board (https://www.surveymonkey.com/r/KWZYT57) and they will provide feedback by COB April 30. The group agreed to review the results at the next CVE Board Meeting, on May 1.
- Next Agenda Items for May 1, 2019:
  - Future discussion items
  - Rules revision list
  - Up and Coming Conferences and Key Meetings

Action Items from Board Meeting held on 17April 2019

#	Action Item	Responsible Party	Status	Comments
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.)	Not Started	Assigned 4/17/2019
4.17.2	Readout of conferences the CVE Program participates in or attends. Provide an analysis and benefit of attending. IOT (Jan'19), HIMSS (Feb'19), VRDX (May 2019), PFIRST (April'19),	MITRE (Jo B.)	Not Started	Assigned 4/17/2019
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)	Not Started	Assigned 4/17/2019
4.17.4	Talk to Katie about ICS-CERT becoming a root CNA and schedule a meeting with ICS-CERT.	MITRE (Chris L.)	Not Started	Assigned 4/17/2019
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)	Not Started	Assigned 4/17/2019
4.17.6	Send list of topics for the CNA Summit to CVE Board.	Tod B.	Completed	Sent to CVE Board 4/17/2019
4.17.7	Follow up with Kurt S. about the survey results; obtain for future use in QWG.	MITRE (Chris C.)	Not Started	Assigned 4/17/2019
4.17.8	Reach out to GitHub about starting the on-boarding process.	MITRE (Jonathan E.)	Not Started	Assigned 4/17/2019

Board Decisions

- CSA working group activities will move to the QWG.

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.

10) Discuss how we can better handle the international community (English requirements of Guidance, Documentation, CVE IDs)