CVE Board Meeting – 15 May 2019

Tod Beardsley, Rapid7
William Cox, Synopsys, Inc.
Kent Landfield, McAfee
Art Manion, CERT/CC (Software Engineering Institute, Carnegie Mellon University)
Beverly Miller, Lenovo Group Ltd.
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
Jo Bazar
Chris Coffin
Christine Deal
Jonathan Evans
Chris Levendis
Lew Loren
Joe Sain
Donna Trammell

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
- *Cloud Security Alliance (CSA)*– Kurt Seifried
- *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 1 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: Approval received for the 20 year celebration at Blackhat USA, in Las Vegas. See open discussions for additional information.
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	5/15 Update: Will coordinate with Microsoft and the MITRE GitHub following the CNA Summit.
3.20.11	Review alternatives for public facing CVE Board discussion group archives.	MITRE (Joe S.)	In process	5/15 Update: Progress on this task delayed due to CNA Summit planning; will re-visit last week of May.
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 (Include 3rd vulnerability summit May 2019)	MITRE (Jo B.)	In Process	5/15: Draft list sent to CVE Board on May 10th. 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
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.
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: Kurt sent an email on 5/13 suggesting that the survey be closed and published as they 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: Waiting on survey to close in item 4.17.1.

Working Group Updates

- CNA Coordination Working Group (CNACWG): Tod Beardsley/Chris Coffin
  - CNACWG met on Wednesday, May 8. The meeting was relatively short because the CNA Summit agenda is completed. Received information on CNA rules revision that is due October 1, 2019. The next CNACWG meeting is scheduled for Wednesday, June 5, 2019.
- Quality Working Group (QWG): Dave Waltermire/Chris Coffin
  - QWG met on Thursday, May 2. Mark Cox with Apache will be the next interview, on Tuesday, May 28, at 11:00am ET. The group talked about the changes to INC3, proposed by Lisa Olson. The slide deck was sent out for review and feedback. Next meeting is Thursday, May 16, at 1:00pm ET.
- Cloud Security Alliance Working Group (CSAWG)
  - Kurt recently sent email to the list stating that the survey should be closed and published as there have been no new results since May 2. A CNA Rule change is being discussed in the QWG to allow vendor CNAs to assign for their own SaaS products.
- Automation Working Group (AWG) – Lew Loren

    - AWG met on Monday, May 13. Continuing progress on the existing three services: CVE ID Allocation, CVE User Registry, Credentialing, Authentication, and Authorization Services
    - CVE ID Allocation Service is the most mature, putting together use cases that cut across all three services and facilitate building out the services in parallel. Early last week, we received the first working skeletal version of the ID Allocation Service; the basic functions are in place.
    - The AWG will continue to provide updates on progress with the services.
    - CVE ID Allocation Service code has been uploaded to GitHub and shared with the AWG.
        - The code can be accessed on the CVE website under AWG links→ https://cveproject.github.io/docs/
    - We are close to having the CVE User Registry and Credentialing, Authentication, and Authorization Services and will be pushing codes as well.
    - Chandan Nandakumaraiah (Juniper Networks) provided an overview of Vulnogram. The AWG plans to leverage the functionality provided in the Vulnogram code in the services development.
    - CVE Website: The current website infrastructure will be replaced with a new platform, which will enable us to field a modern user interface and additional live content capabilities. The website will be created under the Creative Commons Zero (CC0) license.
- Strategic Planning (SPWG) – Kent Landfield/Chris Coffin
    - SPWG met on Tuesday, May 15. The group has completed the Root CVE Numbering Authority (CNA) Roles and Responsibilities Overview deck and has begun turning the deck into prose.
    - The plan is to have a document available to hand to a new Root so they understand their roles and responsibilities and to help them decide if they want to be a Root.
    - The SPWG discussed identifying the next role to target for documentation, with a focus on the roles under the hierarchy so there is a more holistic picture.
    - There was a discussion on authorized data publishers and CNAs, including how they would interact with a Root or sub-root.
    - The group also talked about the updates to be provided at the CNA summit.

CNA Updates

- MITRE – Jonathan Evans
    - Organizations in on-boarding process
        - Met with a potential CNA recruit; it went well, and we are waiting on their example answers.
        - Met with GitHub; they would like to act as a CNA for Git products and assign for repo owners if the repo has vulnerability. They will not be taking assignment requests from 3rd parties; it must be the owner of the repo.
        - Scheduling a McAfee onboarding refresher session for McAfee staff who are unfamiliar with the CNA process.

    - Removals
        - Netgear was removed as a CNA (per their request).
    - Other News
        - CNA1 no longer has a disclosure policy or advisories posted. Jonathan is following up.
- JPCERT - Takayuki Uchiyama
    - No Updates

Open Discussion Items

- **CVE 20 Year Celebration – Chris Levendis**
    - The project has received approval for the 20 year celebration (150 people) at Blackhat USA, in Las Vegas. The group agreed to invite former CVE staff and asked the group to think about CVE stories/war stories to present at the CVE celebration. Next steps are to determine the date of the event and to firm up the contract with the hotel and other logistics. We plan to invite potential Root CNAs and use this as an opportunity to recruit and promote the program. Lisa suggested an award ceremony for "Best" CNA, to use the event as an opportunity to recognize CNAs.
- **Vulnerability Reporting and Data exchange, Special Interest Group (VRDX SIG) – Art Manion**
    - Art explained that, within FIRST, there are multiple special interest groups; the VRDX SIG is one. The original purpose of the VRDX-SIG was a more global look for vulnerability information systems, formats and severity. The structure was born from NIST, CVE, US Government, and software assurance conversations.
    - The 3rd workshop will be a 2-day workshop on May 20 and 21, in Arlington, VA.
        - The topic of this summit is Universal Vulnerability Data Objects, what does a vulnerability data record look like, could there be a standard global record, etc.
        - Kent, Art, and Jonathan Evans will be attending and representing CVE.

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 15 May 2019

#	Action Item	Responsible Party	Status	Comments
5.15.1	Meet at CNA Summit to create the invitation list for CVE celebration	ALL	Not Started	Assigned 5/15/2019

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.

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