CVE Board Meeting – 9 January 2019

Board Members in Attendance

Andy Balinsky, Cisco Systems, Inc.

Mark Cox, Red Hat, Inc.

William Cox, Synopsys, Inc.

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

Kathleen Trimble, U.S. Department of Homeland Security (DHS)

Members of MITRE CVE Team in Attendance
Jo Bazar
Chris Coffin
Jonathan Evans
Joe Sain

Agenda

Introductions, action items from the last meeting

Working Groups

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

CNA Update

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

Open Discussion – Board

Action items, wrap-up

Review of Action Items from Board Meeting held 12 December 2018

- *Previous Action Item:* The MITRE CVE team will discuss with their lawyers the impact of GDPR on the CVE project
    - *Status:* In process
- *Previous Action Item:* MITRE to work with Microsoft on starting the automated submission process (similar to IBM's) and document that process
    - *Status:* Will begin once Microsoft is ready. Targeting February Patch Tuesday based on prior discussion.
- *Previous Action Item:* MITRE (Chris C/Jonathan) to send out an email to the Board list to initiate the CNA Rules revision process.
    - *Status:* In process. We have assembled a list of items and will perform internal review before sending to the Board in Jan. Will also target discussions of these items in the CNA Virtual Summit.
- *Previous Action Item:* MITRE to draft CNA Rules regarding EOL Scoping issue and Note Field in JSON
    - *Status:* In process. This will be included in the CNA Rules revision list
- *Previous Action Item:* MITRE (Jonathan/Joe) will draft up clarifications to CNA rules on the RBP rules and send to the Board for review.
    - *Status:* In process. This will be included in the CNA Rules revision list
- *Previous Action Item:* Kent Landfield is looking into hosting the 2019 CNA Summit.
    - *Status:* In process. CNA ***Virtual*** Summit will be held in the February 2019 to address pressing issues prior to the ***Face-to-face*** CNA Summit in April/May/June 2019.
        - ***Virtual CNA Summit*** - Proposed dates for the Virtual Summit were sent to CNA members: Feb. 4 – 8th; Feb. 25 – Mar 1st.
        - ***Face-to-face CNA Summit*** - Tentative dates for the Summit were sent to CNA members on 1/9/19: April 1st – 5th; May 15th – 17th; May 22nd – 24th; June 12th – 14th; June 19th – 21st.

- Lisa Olson will reach out to GitHub to and see if they can assist DWF.
    - *Status: In process*
- Lisa Olson will write a note describing the Microsoft Virtual Server 2005 Software EOL issue.
    - *Status:* Done. Got a note from Lisa on this and will include in a future writeup.

Working Group Updates

- *Strategic Planning* – Kent Landfield/Chris Coffin
    - The group agreed to hold off on reviewing the Root CVE Numbering Authority (CNA) Roles and Responsibilities document until there is they have a quorum. The next meeting scheduled for January 18th.

    - The group discussed how sub-CNAs deliver CVE submissions. Some subs send directly to MITRE, while others send to their Root CNA. This is currently a Root CNA decision.
- *Automation* – Chris Coffin
    - Kurt Seifried (CSA) created a draft JSON format for the CVE user. A kick-off meeting for the CVE User Registry project is being scheduled and will be announced in the near future.
- *Cloud Security Alliance* – Kurt Seifried
    - The group is completing a set of deliverables that will be presented to the Board. Kurt is working on a set of scenario questions, which will be distributed to solicit feedback.
- *Quality Working Group (QWG):* Dave Waltermire/Chris Coffin – The QWG Kick-off meeting was announced; proposed dates are Thursday, January 17th and Friday, January 18th.
- *CNA Coordination Working* Group (CCWG): Tod Beardsley/Chris Coffin
    - Tod Beardsley (Rapid 7) will be the chair. A Kick-off meeting is being scheduled.

CNA Updates

- *DWF* – Kurt Seifried
    - DWF announced 2 new Sub-CNAs, Jenkins and PHP.
    - Streamlined the process using the CNA registry format.
    - Kurt explained that he researched Jira ticketing, but the expense of purchasing third party workflow applications have put this effort on hold.
- *MITRE* – Jonathan Evans
    - **Johnson Controls** – MITRE is working with Johnson controls to assist them with understanding counting rules. They should be announced as a CNA soon.
    - **CNCERT** – *S*ubmitted their counting rules assignment from the on-boarding session and we are working on reviewing and provided them feedback soonest.
    - Several CNAs have asked for 2019 CVE IDs, but they have outstanding Reserved But Public 2018 CVEs. This has been pointed out and CNAs have submitted updates. There are, however, some continued issues with these submissions.
    - **Apple** – Met with Apple last week, they have agreed to submit their outstanding RBPs by early February. CVE IDs 2019 will be assigned once the RBPs have been resolved.
    - **CY18 Q4 Report card** - Working on the CY18 Q4 Report card for presentation to the Board on January 23, 2019.
- *JPCERT* – Chris Coffin
    - A meeting is being scheduled with JPCERT to discuss their CNA Root status.

Open Discussion Items

- Art attended an OASIS CSAF meeting, in which CVRF was discussed. There was a request for CVRF to support the creation of CVE submissions. It appears that vendor name, product name, and version string are not strictly required by the CVRF format, which is an issue since these data elements are required by the JSON format for CVE entries.

Meeting Action Items

- Kurt will email the Board a link to the DWF Registry on GitHub.

Board Decisions

- None.

Future Discussion Topics

1) *How can we better communicate our future vision of the CVE program? How can we better market the CVE program and communicate the great changes that are taking shape?*
2) *How do we provide more status information to the public around metrics and ongoing activities we are engaged in?*
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*

    The Board discussed that CNA documentation around roles and responsibilities are needed, current documentation is not clear, CNA assign CVE within their scope. Scope may or may not cover CVE for their customers.

    - **CNA Rules -** The rules state CNAs must be responsive but does not provide a specific timeframe. The rules state if a CNA plans to assign a CVE for a vulnerability another vendor's product, to the assigning CNA should contact the vendor. The vendor would then make a determination.
    - **New Approach to CNAs and Roots** - 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 do the CVE assignment as the CNA of last resort.
        - *Action Item* – CNA Rules need to be updated to reflect this new approach.

5) *Eliminate duplication CVE assignment discussion*

- 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 with duplication.
    - **Recommendation 1:** Process recommendation needs to be added to CNA training**.**
    - **Recommendation 2:** CNA rules need to be updated to minimize duplicate assignments.
- Jonathan explained that duplication of CVE assignments occurs the most with DWF.

6) *Researcher CNAs*

- The Board discussed researcher CNAs that have with ambiguous scopes. These CNAs have issued thousands of CVEs.
    - **Recommendation 1:** Avoid adding any new researcher CNAs until there are specific qualifications and guidelines for what qualifies as a researcher CNA. This includes defined scope rules yet to be discussed.
    - **Recommendation 2:** Make the scope naturally programmatic for researcher CNAs.
    - **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 an CVE ID.
    - **Recommendation 4:** Better define roles and responsibilities for researcher CNAs.
    - **Recommendation 5:** Need to address the researcher CNA ambiguous scope issue before onboarding additional researcher CNAs.
    - **Recommendation 6:** Explore the possibility of researchers participating in the CNA program without becoming CNAs.
    - **Recommendation 7:** Need a testing/certification program for CNAs to make sure they can adequately perform their role, especially researchers.
- The Board agreed to explore better solutions regarding the researcher CNA ambiguous scope issue.

7) *Operationalize Root CNAs effectively*
    - Further discussion is needed regarding how we can operationalize Root CNAs more effectively.
    - Additional discussion regarding MITRE's role in operationalizing roots is needed.

8) *Product Type Tagging/Categorization*
    - As the production numbers for CVEs go up, there will be an increasing need to view a subset of the overall CVE master list
    - Define a list of common product areas/domains to be used for categorizing CVE entries (e.g.., Medical devices, automotive, industrial, etc.)
    - The tags/categories should be attached to the products and not to the CVE entries directly.
    - Product listings in CVE User Registry would be a potential location.
    - Can it be automated?

9) *Future of CVSS*
    - Assigning multiple CVSS to a single CVE.
    - Hill discussions around CVSS.