CVE Board Meeting – 12 December 2018

Board Members in Attendance

Andy Balinsky, Cisco Systems, Inc.
Scott Lawler, LP3
Beverly Miller, Lenovo Group Ltd.
Scott Moore, IBM
Lisa Olson, Microsoft
Kurt Seifried, Cloud Security Alliance

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

Agenda

Agenda

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

2:15 – 2:30: Working Groups

- *Strategic Planning* – Kent Landfield/Chris Coffin
- *Automation* – Chris Johnson
- *Cloud Security Alliance* – Kurt Seifried

2:30 – 2:45: CNA Update

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

2:45 –3:15: DWF Root CNA Status and way forward – Chris Coffin, Kurt Seifried

3:15 – 3:45: Software End of Life (EOL) and CVE assignment – Chris Coffin, Lisa Olson

3:50 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held 28 November 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 Dec
- *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 Virtual Summit.
    - *Status:* In process. CNA Virtual Summit will be held in the January/February timeframe to address pressing issues prior to the face-to-face CNA Summit in March/April 2019, which TrendMicro has offered to host. The prospective dates for CNA Summit are March 18 – 22 and April 1 – 5.

Working Group Updates

- *Strategic Planning* – Kent Landfield/Chris Coffin
    - **Strategic Planning Working group:** Discussion at the SPWG centered on upcoming conferences and the potential for CVE outreach opportunities. The SPWG will assist in generating ideas for outreach, participation in general talks, and using security podcast interviews as a method of outreach.
    - **Quality Working group:** The QWG will be co-chaired by Chris Coffin and Dave Waltermire, with a kickoff meeting scheduled for December 19th. The group will focus on best practices and the quality of CVE entries.
    - **CNA Coordination Working Group**: The CCWG has been announced. Tod Beardsley from Rapid 7 has offered to chair or co-chair the group. A slide deck describing Root CNA roles and responsibilities is currently being developed. This presentation describes the need for Root CNAs and their common functions, responsibilities, and requirements.
- *Automation* – Chris Coffin
    - The following projects have been initiated:
        - **CVE ID Allocation Project** – Schmitty (Microsoft) is gathering technical requirements and understanding the specifics of the project. The group has been meeting weekly and is making good progress. Lew Loren from

MITRE has joined the team as a technical project manager and senior developer.
    - **Credentialing, Authentication, and Authorization Project –** Lew Loren and Anthony Singleton (MITRE) developing an initial project description, and a kickoff meeting will be announced in the near future.
    - **CVE User Registry Project –** A kickoff meeting is being scheduled and the search is on for additional participants.
- *Cloud Security Alliance* – Kurt Seifried
    - The CSA is developing a CVE weighting and dimension document, which will be presented to the Board in January 2019.

CNA Updates

- *DWF* – Kurt Seifried
    - No update.
- *MITRE* – Jonathan Evans
    - MongoDB became a CNA on December 10th.
    - Onboarding training with ABB was held on 12/13/18. We expect them to be brought on board quickly.
    - Google Chrome reached out to the CNA Coordinator list this week; they will clear out their RBPs by the end of the year.
    - JPCERT expressed a desire to relinquish their Root CNA role. MITRE will reach out to JPCERT directly to understand the issues regarding this proposed change in status.

DWF Root CNA Status and way forward

- DWF, created by Kurt Seifried, was incorporated into the CVE program as the first Root CNA. Kurt has done a tremendous job with DWF, which supports the entire Open Source community. Unfortunately, DWF is a victim of its own success and has grown to the point that a single person can no longer manage it.
- The Board agreed to think of ways to Federate the program and get additional help for supporting Open Source products. Lisa Olson will follow up with GitHub to see if they can provide some assistance.
- The Board also discussed how the Root CNA role could be improved. Possible areas to consider include: incorporating process automation, developing a scalable ticketing system, and improving format requirements for submission to DWF.

Software End of Life (EOL) and CVE assignment

- MITRE recently received a request from a researcher for Microsoft Virtual Server 2005, a product that reached End of Life status in 2008. Microsoft rejected the request because the product is EOL. The researcher then escalated the request for a CVE to MITRE.
- Lisa Olson noted that the researcher found the issue 10 years ago, and never reported it.

- Kurt added that the researcher is responsible for demonstrating that the vulnerability is valid before any action is taken.
- Lisa will draft up issue and send to MITRE for discussion at a future Board meeting.
- Board members had a range of opinions on EOL products. It may be the case that a Board vote will be required on whether CVEs should be issued for EOL products.
- Language on how EOL products will be handled by CVE will also need to be developed.

Open Discussion Items

- None.

Meeting Action Items

- Lisa Olson will reach out to GitHub to and see if they can assist DWF.
- Lisa Olson will write a note describing the Microsoft Virtual Server 2005 Software EOL issue.

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.