CVE Board Meeting – 28 November 2018

Board Members in Attendance

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)
Ken Williams, Broadcom Inc.

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

Other Attendees
Chris Johnson (NIST)

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: CVE Team Web Scraping – Chris Coffin

3:15 – 3:50: Open Discussion – Board

3:50 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held 14 November 2018

- Action Items: The MITRE CVE team will discuss with their lawyers the impact of GDPR on the CVE project
    - *Date assigned:* 10/31, to Chris Coffin
    - *Status:* In process
- *Action Item:* MITRE to work with Microsoft on starting the automated submission process (similar to IBM's) and document that process
    - *Date assigned:* 10/31, to Chris Coffin
- *Status:* Will begin once Microsoft is ready; estimated start date is February 2019. *Action Item:* Dave Waltermire to set up a conference call to get feedback on the Vulntology
    - *Date assigned:* 10/31, to Dave Waltermire
    - *Status:* Vulntology Google Group established; conference call to be scheduled soon.
- *Action Item:* MITRE to send out an email to the Board list to initiate the CNA Rules revision process.
    - *Date assigned:* 10/3, to Chris Coffin & Jonathan Evans/Joe Sain
    - *Status:* In process. A list of items has been developed and will be sent to the Board following internal review.
- *Action Item:* Send out note to Board on CVE Quality WG
    - *Date assigned:* 10/3, to Chris Coffin
    - *Status:* Done. The new WG will be established and the initial meeting will take place in early December.

Working Group Updates

- *Strategic Planning* – Kent Landfield/Chris Coffin
    - *Strategic Planning Working Group* met on Monday, November 26th.
    - Quality Working Group was initially introduced to the SPWG by Jonathan Evans to address the quality of CVE descriptions. Since that time, the scope of the Quality WG scope has expanded to include CVE output as a whole:
        - What does CVE look like to consumers?
        - How do they use the data?
        - What elements are most important?
        - What are the trade-offs between speed and quality?
        - Should we revisit the content of CVE entries, including the minimum required data, etc.?
    - Bank of America is interested in participating in the CVE program. They participated in the Automation Working Group meeting this week. Chris believes this would help add consumer perspective in the Quality Working Group.
    - Dave Waltermire, Kent Landfield, Chris Johnson, Chris Levendis, and Chris Coffin offered to participate in the Quality WG as co-Chairs.

    - The SPWG continued the discussion on the responsibilities of Root CNAs with an eye to more tightly defining those responsibilities. Results of this work will be presented in the near future.
- *Automation* – Chris Johnson
    - The Automation Working Group met on Monday, November 26th.
    - The AWG identified a set of high-level topics for future meetings:
        - Cross-cutting issues
        - High-level work flows
        - Identifying the dependences that exist between the services being worked by the project teams
    - The AWG will also study the privacy and security issues surrounding the data that will be collected, which will help with future scope discussions.
    - *CVE ID Allocation Service*
        - At the most recent requirements meeting, attendees identified a number of use cases and began to drill down into CVE attributes.
        - Schmitty, the CVE ID Allocation Service lead, will post the meeting notes to the project GitHub site, located at: https://github.com/CVEProject/CVE-ID-Allocation-Service
        - The group also discussed capturing CNA profile information, including the number of CVE IDs, basic attributes of CNAs that would be stored in a repository.
        - Chris Coffin advised the group that any proposed changes to rules and processes must go through the SPWG and Board for review and approval.
    - Chris Coffin advised the Board that a new MITRE team member, Lew Loren, is joining the CVE project. Lew will lead the implementation of the new content production system and will be a liaison between the CVE Working Groups. He will take on a technical advisory role for AWG development projects and will lead the Credentialing, Authentication, and Authorization project.
- *Cloud Security Alliance* – Kurt Seifried
    - The CSA group is reviewing use cases and the CVE value proposition. CSA is hearing from some organizations that CVE for Services is a bad idea. It appears that some of the cloud service providers do not want the additional overhead of providing CVEs for their services, and in some cases do not want the additional visibility of publicly announcing vulnerabilities.
    - CSA has also been looking at the possible modification of Inclusion Rule 3. Currently, CVE does not officially cover hardware or cloud services. The board will have to make a discussion on whether to expand CVE to these areas.
        - Board members felt that if there was an issue that was internal facing and had no user impact or user action required, a CVE may not be necessary. It is important to clearly define what gets a CVE.
    - Kurt feels that the CVE for Cloud Services group has done all that they can do within the confines of the current CVE scope. There are cloud service organizations that believe that CVEs for services are necessary, and there are cloud service organizations who do not. The group has defined the problem space well.

- Dave added we should look at identifying different classes of CVEs, so they can be filtered and allow CNAs the flexibility.
- If there is a meaningful group of cloud service providers and consumers that feels that CVEs for services is important, we should explore a way of piloting support for this sector.
- Kurt will produce a document that defines the problem and presents possible solutions. Kurt will send this document to the Board for review in January 2019.
- Microsoft's reticence is that they do not want to devalue CVE by assigning IDs to everything regardless of whether there is action or no action. Microsoft does not want to be in the position of having to evaluate every request for a flood of new service CVEs that may have no user impact.

CNA Updates

- *DWF* – Kurt Seifried
  - DWF has cleared up their CVE assignment backlog.
  - A meeting with the CVE team is scheduled for December 5th to discuss streamlining the CNA process.
- *MITRE* – Jonathan Evans
  - Johnson Controls has nearly completed the CNA onboarding process.
  - ABB CNA onboard session scheduled on December 11th
  - BugCrowd requested to be a CNA. MITRE has asked for additional information from BugCrowd. This is their 3rd request; the two previous engagements were not completed on the BugCrowd side.
  - Another researcher requested to be CNA; we have put a hold on new researcher CNAs at the request of the Board.
  - We are working through some issues with the Intuit request and we are making progress.
  - Getting request for 2019 IDs but some CNAs have RBP's that need to be cleaned up before new IDs can be issued.
  - SUSE and Microfocus announced that they are going to split into separate companies and that they want to be separate CNAs.
- *JPCERT* – Taki Uchiyama
  - JPCERT expressed that they do not have an interest from vendor CNAs, and they would like to be removed from Root CNA status at this time. If they do receive interest from vendor CNAs, they would like to be able to restart Root CNA status.
    - Board had no issue with this change.

CVE Team Web Scraping

- The objective of increasing CVE web scraping is to address the perceived gap in lack of CVE coverage.

- MITRE and DHS want to address the gap by enhancing up the web scraping process.
- We plan to find source information in areas of IT that CVE has not been able to cover through traditional means.
- We would identify the resources to use and automate the scraping process and populate the CVE IDs.
- A suggestion was aired to make URL-Only CVE IDs, instead of the traditional description/content part of the ID to speed up the consumption and creation. Other members suggested that this would lead to less useful CVEs.
- Chris C. noted that the Board may need to revisit the CVE ID requirements.

Open Discussion Items

- None

Meeting Action Items

- Kent Landfield is looking into hosting the 2019 CNA Summit; MITRE will follow up with Kent.
    - Agenda item: CVE for services, include governance

Board Decisions

- VOTE: Kathleen Trimble CVE Board Membership

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.