CVE Board Meeting – 31 October 2018

Board Members in Attendance
Andy Balinsky, Cisco Systems, Inc.
Kent Landfield, McAfee
Scott Lawler, LP3
Art Manion, CERT/CC (Software Engineering Institute, Carnegie Mellon University)
Pascal Meunier, CERIAS/Purdue University
Lisa Olson, Microsoft
Kurt Seifried, Cloud Security Alliance
David Waltermire, National Institute of Standards and Technology (NIST)
Ken Williams, CA Technologies

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* – Chris Coffin
- *Automation* – Chris Johnson
- *Cloud Security Alliance* – Kurt Seifried

2:30 – 2:45: CNA Update

- *DWF* – Kurt Seifried
- *MITRE* – Jonathan Evans
- *JPCERT* – No Update

2:45 –3:50: Open Discussion – Board

3:50 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held October 17, 2018

- *Previous Action Item:* MITRE to create Q3 report card slide deck with CNA-specific slides removed
    - ***Status:*** Done; will be distributed to the Board
- *Previous Action Item:* MITRE (Chris Coffin/Jonathan Evans) to send out an email to the Board list to initiate the CNA Rules revision process.
    - ***Status:*** In process
- *Previous Action Item:* MITRE to draft CNA Rules regarding EOL Scoping issue and Note Field in JSON
    - ***Status:*** Not done
- *Previous Action Item:* Kurt Seifried to provide CVE User Registry project participants
    - Kurt has identified a number of potential participants. Kurt will change the process for the DWF registry. Currently, there are separate CNA and CV Mentor registries; these will be merged together and will form a prototype CVE User Registry for the Automation Working Group project.
    - Due to potential issues with GDPR, DWF will also reduce the amount of personal information that is required for registration. DWF will no longer require people to send a copy of their GPG key but it will require them to send their finger print and upload their key to the SKS server. Kurt is looking at other ways to avoid collecting PII; if PII is required, DWF will not host it.
    - **GDPR concerns also bring up the issue of whether CVE should use GitHub to store information.** GitHub and Microsoft do not want to spend a lot of time dealing with GDPR. Microsoft and GitHub requested that Kurt meet with their lawyers to discuss the issues he is encountering. Kurt will keep the group posted.
    - The two main issues with GDPR are the availability of PII (e.g., Emails, company names) and whether that information is publicly available. The Board would like MITRE's lawyers to provide them with guidance on GDPR. The Board will need assistance to understand what the options are going forward.
- *Previous Action Item:* Send note to Board on CVE Quality WG (MITRE)
    - ***Status:*** Not Done

Working Group Updates

- *Strategic Planning* – Chris Coffin
    - First draft of the Authorization, Credentialing, Authentication Services document was sent out for SPWG review in early October. The kick-off meeting for the CVE ID Allocation service is scheduled for November 6th. Topics for future Strategic Planning Working Group meetings were identified as ideas for new funding models, CNA of last resort, and Root CNA.
- *Automation* – Chris Johnson
    - Discussed GDPR issues with the group.

    - Proposed date has been set for the kickoff of the CVE ID Allocation Service (Nov. 6).
    - Microsoft expressed interest in participating in the automated submission pilot.
        - Currently, there is no documented step-by-step process for allowing automated submissions, and one should be developed. Microsoft has offered to assist with this task; MITRE has the action to document the process.
- *Cloud Security Alliance* – Kurt Seifried
    - Kurt discussed how the use cases around CVE for services has revealed some blind spots. Before moving forward with service CVEs, the following must be defined:
        - What is a vulnerability in a services context?
        - What is an exposure in a services context?
    - The next CSA meeting will involve a discussion of a framework to identify different vulnerabilities and who is responsible for fixing them.

CNA Updates

- *DWF* – Kurt Seifried
    - No Updates
- *MITRE* – Jonathan Evans
    - Logitech contacted us to be a CNA, and Johnson Controls will be submitting their CNA registration information by the end of the week. IBM announced the intent to acquire Red Hat; it is unclear how this will impact the CNAs for either company. Once the acquisition is final, MITRE will follow up with IBM and Red Hat CNAs.
- *JPCERT* – Taki Uchiyama
    - No updates

Open Discussion Items

- **CVSS scoring and assigning multiple scores to different products for the same vulnerability:** Art Manion (CERT/CC) walked through an example: When there is a CVE ID that affects core browsing code, the Edge browser on Windows 10 should have a different CVSS score than Edge on Windows server, since the default configurations are different, and Windows server has better sandboxing capabilities. The question is, how should CVSS point to the CVE ID? Kurt noted that this is supported in the JSON.
- **CVSS SIG Meeting update:** Art Manion reported that the SIG group is working on a CVSS 3.1 release, with plans for future minor releases.
- **OASIS CSAF Update:** Art Manion attended the OASIS telecon in which changes to the CVRF specification were discussed. The group is working on a JSON version for their next release. The CVE format was a topic of discussion, and CSAF is aligning their formats with CVE formats.

- **Vulntology**: Dave Waltermire provided an update: NIST solicitated the community for comment on the Vulntology, but they have not received any response to date. Dave suggested that setting up a conference call to get feedback, as well as establishing a Google group to stimulate more conversation and to obtain feedback.

Meeting Action Items

- The MITRE CVE team will discuss with their lawyers the impact of GDPR on the CVE project.
- MITRE to work with Microsoft on starting the automated submission process (similar to IBM's) and document that process.
- Dave Waltermire – Set up a conference call to get feedback on the Vulntology.
- MITRE will distribute a scrubbed version of the Quarterly Report Card for Board review.
- MITRE will develop a step-by-step process document for joining the GitHub Automated Submission process with Microsoft in December.

Board Decisions

- The Board agreed to add Microsoft to the GitHub Automated Submission process.

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.

Meeting recordings available here:
https://handshake.mitre.org/file/view/15218030/cve-board-meeting-10-17-18-part-1
https://handshake.mitre.org/file/view/15220827/cve-board-meeting-10-31-18-part-2