CVE Board Meeting – 14 November 2018

Board Members in Attendance

Andy Balinsky, Cisco Systems, Inc.
Mark Cox, Red Hat, Inc.
William Cox, Synopsys, Inc.
Scott Lawler, LP3
Beverly Miller, Lenovo Group Ltd.
Scott Moore, IBM
Lisa Olson, Microsoft
Takayuki Uchiyama, Panasonic Corporation

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

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* – No meeting this week
- *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: CNA Rule modification discussion: Reserved but Public (RBP) – Jonathan Evans

3:15 – 3:50: Open Discussion – Board

3:50 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held 31 October 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:* Coordinating schedules with Microsoft
- *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; Doodle Poll sent on date for conference call
- *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
    - *Status:* In process
- *Action Item:* MITRE to draft CNA Rules regarding EOL Scoping issue and Note Field in JSON
    - *Date assigned:* 10/3, to Jonathan Evans
    - *Status:* Action item will be rolled into CAN Rules Revision process
- *Action Item:* Send out note to Board on CVE Quality WG
    - *Date assigned:* 10/3, to Chris Coffin
    - *Status:* Not done

Working Group Updates

- *Strategic Planning* – No meeting this week
- *Automation* – Chris Johnson
    - Kickoff meeting was held on Tuesday, Nov 6th to discuss the CVE ID allocation service requirements.
    - The group discussed possible GDPR impacts to the CVE User Registry service activity.
    - The group is looking for a leader for the Credentialing, Authentication, and Authorization service., A team will be formed to develop the requirements.
    - A kickoff meeting still needs to be scheduled for the User Registry Service requirements meeting; will follow up with Kurt.
- *Cloud Security Alliance* – Kurt Seifried
    - No Update

CNA Updates

- *DWF* – Kurt Seifried
    - No Update
- *MITRE* – Jonathan Evans
    - Received one new CNA request, Resilio. CNA onboarding materials were sent to them.
    - Broadcom completed its acquisition of CA. CA contact information has been updated, although it is unclear if they will remain a CNA. We will monitor the situation.
- JPCERT – Taki Uchiyama
    - We had a meeting with JPCERT about their status as a root CNA and a follow up meeting has been scheduled next week, to get their final decision on whether they wish to continue to be a root CNA.

Open Discussion Items

CNA Rule modification discussion: Reserved but Public (RBP) – Jonathan Evans

- CNA rules are vague regarding when a CNA is responsible for submitting an entry; the rule can be interpreted many ways.
    1. One interpretation is that the CNA is required to submit an entry once the CNA published an advisory about the vulnerability,
    2. A second interpretation is that, the CNA is responsible for submitting the entry regardless of the source of the public advisory.
- In September, a new policy was implemented, which states that if a CNA has Reserved but Public (RBPs) IDs, no new CVE IDs will be issued. For example, if a researcher publishes an advisory before a CNA is ready to publish, should we consider this an RBP and block the issuance of new CVE IDs?
- Mark Cox discussed his experience with this new policy when Apache requested 2009 CVE IDs and was rejected because a researcher had published an advisory prior to coordinating with Apache.
- The frequency of the problem was discussed. It is relatively infrequent, but it can happen more often with distributed projects like Apache.
- Lisa Olson (Microsoft) explained they sometimes provide CVE IDs to researchers prior to patch Tuesday, but they tell the researcher they cannot go public with the CVE ID prior to the release of the documentation from Microsoft. If a researcher was to go public prior to Microsoft's release of the documentation, Lisa's position is that they will not talk about it publicly until Microsoft releases the CVE ID.
- Mark Cox also brought up the possibility of releasing a "stub" entry that lists a vulnerability with limited information, which would be expanded at a later date. According to the current rules, this is not enough to unblock the release of additional IDs.

- The group agreed that the rules should clearly specify when publication should happen, and perhaps there should be a limited exception in cases such as those that have been discussed.

Meeting Action Items

- MITRE will draft clarifications to the RBP rules and send to the Board for review.

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.