CVE Board Meeting – 3 October 2018

Board Members in Attendance

Mark Cox, Red Hat, Inc.
William Cox, Synopsys, Inc.
Kent Landfield, McAfee
Scott Moore, IBM
Lisa Olson, Microsoft
Kurt Seifried, Cloud Security Alliance
Takayuki Uchiyama, Panasonic Corporation
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 – Chris Coffin

2:15 – 2:30: Working Groups

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

2:30 – 2:45: CNA Update

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

2:45 – 3:00: Board Homework: How to advertise CVE Metrics to the Community – Board Discussion

3:00 – 3:30: Scoping as it relates to the CVE User Registry – Kurt Seifried

3:30 – 3:50: CVE assignments for end of life and unsupported products – Chris Coffin

3:50 – 4:00: Action items, wrap-up – Chris Coffin

Review of Action Items from Last Meeting – 19 September 2018

- *Previous Action Item:* Art Manion to report back to the Board about the CVSS SIG Meeting
    - *Status:* Not Done
- *Previous Action Item:* Scott Moore to notify MITRE on how to handle IBM researcher CNA status
    - *Status:* Complete – Asked and received a new of Block of CVE IDs.
- *Previous Action Item:* MITRE to add Andy Balinsky to the Cloud Security Alliance working group to discuss CVE for services
    - *Status:* In process
- *Previous Action Item:* Andy Balinsky - Post message/document to the list as a foundational piece regarding Cloud Security Alliance.
    - *Status:* Complete
- *Previous Action Item:* MITRE to add CSA to the regular Board meeting agenda
    - *Status:* Complete
- *Previous Action Item:* Kurt Seifried to provide the names of those participating in the CVE User Registry project and set up a requirements kickoff meeting.
    - *Status:* Not Done
- *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
- *Previous Action Item:* Send out note to Board on CVE Quality WG (MITRE)
    - *Status:* Not Done

Working Group Updates

- *Strategic Planning* – Kent Landfield / Chris Coffin
    - Meeting held on Monday, October 1, 2018. The group continued the discussion on ROOT CNAs roles and responsibilities. Continued with developing additional questions to help identify roles and responsibilities
    - MITRE has action items to update the Questionnaire we send to CNAs, for ROOT CNA and send to SPWG for input/feedback.
- *Automation* – Chris Johnson / Dave Waltermire
    - Meeting held on Monday, October 1, 2018. The Doodle Polls are out to the SWG for setting up the Kick-Off Meetings for each of the current requirements projects.
    - Chris Johnson explained he is looking for someone on the SPWG to help facilitate the initial walk thru of the service document, communicate the vision and get the team up to speed. He is also developing requirements in use case boiler plates, so we can write the requirements.

    - Kurt reported about working toward changes to the JSON format for the user registry and discussed more about scope statements (added topic to this Agenda item)
    - Chris Coffin advised the group that initial draft of the Credentialing Authentication & Authorization Document and will be distributed to the SPWG in the next few days.
- *Cloud Security Alliance* – Kurt Seifried/Chris Coffin
    - The group went through Counting and Inclusion rules, reviewing what should and should not be changed. The group agreed that changing as little possible is the goal and not to have special rules (i.e. Services, IoT, Medical devices, etc.)
    - The group discussed what to do with IN3.0, modify or remove it and CN2.1, discussed dispute resolution and vendors not behaving well.
    - The participation for Services CNA will be OPT-IN only to start.
    - The group still needs to determine if it would be beneficial and is there a workable solution for identifying Cloud Services vulnerabilities.

CNA Updates

- *DWF* – Kurt Seifried
    - GitHub is CNA for their own software, they want to be a Community CNA for content living in GitHub. GitHub would like to identify security issues/ vulnerabilities and be able to report and fix vulnerabilities in their infrastructure.
    - Kurt explained he is working with GitHub on researching and developing a roadmap on what a Community CNA process would look like. There is a lot more details to work out before being able to present this to the board.
    - Kurt explained to GitHub the idea of 3rd party CNAs for vendors is to give the vendor the first right of refusal.
    - GitHub is putting together a cover letter to present to the Board.
    - The Board expressed concern about how the acquisition of GitHub by Microsoft could have a significant impact on this process
        - Kurt is reaching out to GitHub POC and providing them with contact information for Lisa Olson (Microsoft).
- *MITRE* – Jonathan Evans
    - No updates
- *JPCERT* – Taki Uchiyama
    - No updates but Taki did visit the office to get a feel for how the turnover of staff has impacted their resources for outreach and their ability to fulfill their commitment as a Root CNA. JPCERT is currently understaffed and is unable to onboard CNAs, but they can report CVEs.
    - The group discussed changing their status of Root CNA temporarily.
    - Taki has an action item to follow up with JPCERT about this temporary status change.

Open Discussion Items

- **Board Homework: How to advertise CVE Metrics to the Community** – Board Discussion
    - Chris Coffin suggested to include the basic information, number of CVE ID and Populated by year, average time to reserve, to populate, and so on.
    - Kent suggested removing CNA specific graphs and using slides from the CVE Quarterly Metrics Report as the baseline for the CVE Metrics.
    - The Board will review the Q3 Report Card (Exclude CNA specific info) in the next meeting, October 17th.
- **Scoping as it relates to the CVE User Registry** – Kurt Seifried
    - See below
- **CVE assignments for end of life and unsupported products** – Chris Coffin
    - Kurt explained his view point on the EOL scope issue:
        - IF a CNA has a specific scope that does include EOL products, if they don't explain it clear enough, they must live with the consequences.
        - IF CNAs choose not to participate, then the issue gets escalated to the Root CNA.
    - Chris Coffin explained that examples would be helpful for the CNAs as to what are good scopes compared to bad scopes.
    - The group discussed that the scope should include a turn-around time that the Vendor CNA needs to respond to the Parent CNA, when time is up, the Parent CNA will report the CVE.
    - Jonathan explained that MITRE should disclose the policy for handling EOL issues moving forward, so that it is clear to CNAs how MITRE handles them.
    - Kurt wants the CNAs to make clear in their scope declarations that EOL are covered or not covered. The group agreed that vendors find it very difficult to keep up the EOL list, to keep it current.
        - Kurt explained that not all Vendors get back to him about whether a product is EOL.
    - Lisa Olson suggested that CNAs should alert their parent CNA if they choose not to make a CVE assignment.
    - Kurt explained that he would like the Vendors to determine their level of participation.

    Chris asked the Board the following questions:

    1. **Is it the responsibility of Parent CNA/MITRE if the scope of the Vendor CNA is clear (that EOL is out of scope), should MITRE have to go back to the Vendor CNA to let them know we are creating a CVE for an EOL product?**
        - The group agreed reaching out to the Vendor CNA would not be necessary, if it's specifically out of scope. However, if the scope says everything is covered, then the Vendor CNA decides if they want to cover it, otherwise it gets escalated to the Parent CNA.
    2. **Does everyone agree that a CVE should be assigned if a product is EOL and a valid vulnerability?**

- Kurt clarified that it should be EOL and currently being used somewhere (i.e. something that was assigned EOL yesterday)?
- Chris Coffin asked the group how can we determine what is still being used and how do we determine if someone is abusing it?

3. **Should a new tag be created when a product is EOL?**
   - Chris Coffin explained that products change statuses often from In-life or end of life and keeping this up to date, would be unmanageable.

- Further discuss EOL issues, subsequently develop language to address this issue.

Meeting Action Items

- Taki to meet with JPCERT in late October to discuss their Root CNA status
- MITRE to draft CNA rules regarding EOL scoping issues.
- MITRE to draft CNA rules regarding note field in the JSON.
- MITRE to create Q3 report card slide deck with CNA-specific slides removed
- Set up call with the Board to review CVE metrics to advertise to the Community Q3 report card with CNA-specific slides removed
- Art Manion to report back to the Board about the CVSS SIG Meeting
- Kurt Seifried to provide the names of those participating in the CVE User Registry project and set up a requirements kickoff meeting
- Send out note to Board on CVE Quality WG (MITRE)

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.