CVE Board Meeting – 17 October 2018

Board Members in Attendance

Andy Balinsky, Cisco Systems, Inc.
Mark Cox, Red Hat, Inc.
William Cox, Synopsys, Inc.
Art Manion, CERT/CC (Software Engineering Institute, Carnegie Mellon University)
Beverly Miller, Lenovo Group Ltd.
Scott Moore, IBM
Lisa Olson, Microsoft

Members of MITRE CVE Team in Attendance

Jonathan Evans
Joe Sain
George Theall

Other Attendees

Chris Johnson (National Institute of Science and Technology (NIST)

Agenda

Agenda

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

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: CVE Quarter 3 Report Card Slide Deck Review – Board Discussion

3:00 – 3:50: Open Discussion – Board

3:50 – 4:00: Action items, wrap-up

Review of Action Items from Board Meeting held October 3, 2018

- *Previous Action Item:* Art Manion to report back to the Board about the CVSS SIG Meeting
    - *Status:* Art Manion provided an update:
        - Facebook was hacked, and they submitted 3 vulnerabilities in more detail than CERT-CC has ever seen for a service vulnerability.
        - The CVSS group discussed if/how to score them and how to do chaining. Are there CVE IDs for Services?
        - There was a discussion on whether more than one CVSS score can be assigned to one CVE ID.
- *Previous Action Item:* MITRE to create Q3 report card slide deck with CNA-specific slides removed
    - *Status:* In process; Q3 Report Card is on the agenda today
- *Previous Action Item:* MITRE to send a note to the Board on the CVE Quality Working Group
    - *Status:* Not done
- *Previous Action Item:* MITRE 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:* MITRE to add CSA to the regular Board meeting agenda
    - *Status:* Complete
- *Previous Action Item:* Kurt Seifried to provide CVE User Registry project participants and set up a requirements kickoff meeting
    - *Status:* Not Done
- *Previous Action Item:* Send out note to Board on CVE Quality WG (MITRE)
    - *Status:* Not Done

Working Group Updates

- *Strategic Planning*
    - No meeting this week
- *Automation* – Chris Johnson
    - Discussed scheduling the kickoff meetings for the ID Allocation project and the CVE User Registry project. Schmitty from Microsoft agreed to co-lead the CVE ID Allocation Service project with Beverly Miller. Chris Johnson has been working with Kurt Seifried, the CVE User Registry project lead, to get the kickoff meetings scheduled.
- *Cloud Security Alliance* – Kurt Seifried/Chris Coffin
    - Lisa Olson provided an update on the CSA WG. There was a recommendation to review the INC3 inclusion rule. There was a spirited discussion about why removing this inclusion would weaken the value of the CVE and require someone to scrub through the CVE to determine if action is warranted. Discussion on this topic will continue.

CNA Updates

- *DWF* – Kurt Seifried
  - No Update
- *MITRE* – Jonathan Evans
  - Intuit and Tanium have requested to become CNAs.
- *JPCERT* – Taki Uchiyama
  - No Update

Open Discussion Items

- Q3 - Quarterly Report Card review – Jonathan Evans
  - Jonathan walked through the Quarterly report card with the Board Members
  - This report will be used to develop the metrics for the CVE webpage. Board members continue to discuss what metrics should be included for publication.

Meeting Action Items

- None

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.