CVE Board Meeting 4 April 2018

Board Members in Attendance

- Beverly Finch, Lenovo
- Chris Johnson, NIST
- Kent Landfield, McAfee
- Scott Lawler, LP3
- Scott Moore, IBM
- Kurt Seifried, Red Hat
- Dave Waltermire, NIST

Members of MITRE CVE Team in Attendance

- Nicholas Caron
- Jonathan Evans
- Joe Sain
- George Theall

Agenda

2:00 – 2:10: Introductions, action items from the last meeting – Joe Sain

- **Previous Action Item:** Kent Landfield to make minor modifications to the Board Charter regarding proxy voting language and CNA Representative's position.
 - **Status:** Done; sent to the Board list 4/2.
- **Previous Action Item**: Kent Landfield to write a message for the CNA list that describes the CNA Working Group.
 - Status: Deferred until Board Charter modifications are incorporated.
- **Previous Action Item**: We need to think more about the task of defining a draft proposal for CVE language requirements (i.e., should CVE require an English description?). We should develop a lightweight proposal to get the discussion started.
 - Status: TBD.

2:10 – 2:30: Working Groups

- Strategic Planning Kent Landfield
- Automation Chris Johnson, Dave Waltermire, George Theall
- 2:30 2:50: CNA Update
 - DWF Kurt Seifried
 - MITRE Jonathan Evans, Nick Caron

2:50 – 3:00: CVE GitHub landing page and Working Group Repositories – Joe Sain

- <u>http://cveproject.github.io/docs/</u>
- https://github.com/CVEProject/CNA-registry-project-AWG,
- https://github.com/CVEProject/JSON-format-project-AWG

3:00 - 3:30: CVE Working Groups: How should non-Board members or non-CNAs be permitted to participate? – Dave Waltermire

3:30 – 3:50: Open Discussion

3:50 – 4:00: Action items, wrap-up – Joe Sain

Agenda Items

Board Working Groups

Strategic Planning Working Group (Kent Landfield)

ISSUES: Discussion ongoing about roles and responsibilities, more discussion being done on automation administration needs, what needs to be put in place to make roles functional, and role reengineering as a whole. The European Union (EU) General Data Protection Regulation (GDPR), which goes into effect on May 25, 2018, will need to be accounted for in some manner, some disagreement over what direction should be taken with this, (ignore for now, or account for it? Is opt-in sufficient, or is opt-out also necessary [opinion of MITRE lawyers is the latter].). Should all products containing a person's name be outright refused for publication? Cease and desist could have negative effects on the program.

ACTIONS:

- Dave Waltermire: Action item ongoing for automation workflow process.
- Chris Levendis: Action item ongoing for master DB query, download, ID allocation, and entry submission business rules.

These should be done in the next two weeks, RSA permitting.

Conversation of GDPR ongoing.

BOARD DECISIONS:

None

Automation Working Group (Chris Johnson/Dave Waltermire/George Theall)

ISSUES:

Went over outstanding issues for working group charter. Spent some time discussing using GitHub as a collaboration tool. Joe Sain presented the current flat structure for the github io pages for documentation/working group and project repos. Spent some time talking about workflow, issue management, possibly using project board in Github to give better views over issues.

Discussed in the call was a potential need for more effort into nurturing the culture of using Git for CVE, documentation being a good start to this end. Also, should the CVE webform be deprecated, (long off to-do)?

ACTIONS:

- Joe Sain: timeline for defining a common directory structure for storing project artifacts within workgroups.
- Joe Sain: List of repos on GitHub, including working groups and AWG projects, (current WIP)
- Kurt Seifried: Create workflow documentation for using Git and GitHub for submission (this week or before the next board call).

BOARD DECISIONS: None

CNA Updates

DWF (Kurt Seifried)

STATUS: using automatically built descriptions to great success for improving workflow.

ISSUES/DISCUSSION: May be worth building a more general description generation tool to avoid various issues concerning descriptions.

ACTIONS: None

MITRE (CVE Team)

STATUS: CVE is about to bring on SonicWall as CNA, with an announcement planned for Friday. Training for Avaya, Palo Alto Networks, and Taiwan CERT, all within next week or so.

ISSUES/DISCUSSION: Getting close to 100th CNA! It would be worthwhile to have a press release to celebrate/outline the recent accomplishments of the CNA program, at the time of the 100th CNA.

MITRE has been getting a CNA request per week, requiring all CNAs to get trained up, (4-5 hours per), which has been time consuming. Considering creating regular sessions, 1 per everyother week, which anyone (potential CNA or current) can sign up for, with a test for candidates to determine understanding of material.

ACTIONS:

- MITRE: Generate training test documentation. Kent Landfield is willing to review it, and Dave Waltermire is willing to sit in on a session for review.
- MITRE: Once above is done, will be providing CNA training for all interested parties, (both pre-CNA and current CNAs), once every other week.
- MITRE CVE PR: Draft up the press release to coincide with the 100th CNA, gather quotes from various community members on successes of program to that end.

Agenda Items

CVE GitHub landing page and Working Group Repositories: Joe Sain

ISSUES: Mostly covered elsewhere, though looking for feedback on current look and feel! Directory structure formation ongoing.

ACTIONS: None

BOARD DECISIONS: None

<u>CVE Working Groups: How should non-Board members or non-CNAs be permitted to</u> <u>participate?</u> *Dave Waltermire*

DISCUSSION: Chris Johnson is working on project descriptions for WG projects, and once those are complete, we will be looking to bring in hands to work on said projects. Can we bring in outside people to this end? Working group charter says yes.

ACTIONS:

• Bring up concept on bringing in outside people to work on projects to the CNA List. If met with approval, potentially codify in the board charter.

BOARD DECISIONS: None

Open Discussion

CVE ID "OWNERSHIP" TRANSFER:

DISCUSSION: CVE ids may need to transfer "ownership" (which CNA has this id in their block), for a variety of reasons, though this is currently only tracked internally with MITRE due to privacy concerns. A protocol may be necessary for mutual agreement and ID transfer processes. This problem becomes much easier should this be tracked externally and kept in the public CVE data itself, tying back to the Automation Working Group discussion over the publication of ID "ownership" and the resulting abolishment of blocks, (the ID request API replacing block requests).

ACTIONS: None, conversation ongoing.

CVE JSON Modifications to Support NVD:

DISCUSSION: Reference names and sources attributes were added to the JSON schema, which will be going live 4/5/18, unless immediate objections are raised. Discussion concludes a JSON schema should exist to check against NVD data, to ensure validity when provided. MITRE at the current time will only be checking against the minimum schema, (for example, MITRE does not currently validate CVSS scores, if included).

There was a discussion regarding whether there is a need to create another schema file that would allow people to validate their JSON; no action was taken to do so at this time.

ACTIONS: None.

NEXT BOARD MEETING DURING RSA SECURITY CONFERENCE:

DISCUSSION: The Board discussed the fact that the next scheduled meeting falls during the RSA Security Conference and that a number of Board members would be attending the conference.

ACTIONS: Next board meeting rescheduled due to RSA.

BOARD DECISIONS: The Board meeting scheduled for April 18 will be canceled and moved to April 25. The regular bi-weekly board meeting schedule going forward will remain intact, which means that there will be a Board meeting on May2.

Summary of Action Items:

- Ongoing action items for Strategic Planning working group will hopefully be wrapped up in 2 weeks. The European Regulation conversation is ongoing.
- In the Automation Working Group, Joe Sain will continue with the effort to define a proper directory structure for the CVE Project Github.io site for project artifacts, as well as generating a list of all CVE and WG-related repos.
- Kurt Seifried will develop documentation for how to submit via the Git Pilot before the next Board call.
- MITRE will generate test material for CNA training, while also providing said training every other week for CNAs and pre-CNA entities.
- MITRE will generate a draft press release to announce the approaching 100th CNA onboarded, highlighting the growth and improvement of the CVE program as a whole.
- The concept of bringing in outside people to work on working group projects will be proposed to the CNA List. If met with approval, it should be codified in the board charter.