CVE Board Meeting 15 November 2017

Board Members in Attendance

William Cox (Black Duck)
Kent Landfield (McAfee)
Kurt Seifried (Red Hat/DWF)
Pascal Meunier (CERIAS/Purdue University)

Members of MITRE CVE Team in Attendance

Nick Caron
Chris Coffin
Jonathan Evans
Joe Sain
Anthony Singleton
George Theall
Alex Tweed

Agenda

2:00 – 2:05: Introductions, action items from the last meeting – Chris Coffin
2:05 – 2:25: Working Groups
- Strategic Planning – Kent Landfield
  - Issues
  - Actions
  - Board Decisions
- Automation – George Theall
  - Issues
  - Actions
  - Board Decisions

2:25 – 2:50: CNA Update
- DWF – Kurt Seifried
  - Issues
  - Actions
  - Board Decisions
- General – Jonathan Evans, Nick Caron, Joe Sain
  - Issues
  - Actions
  - Board Decisions

2:50 – 3:10: Documentation: CNA Processes – Jonathan Evans
3:10 – 3:30: Discussion: Problematic assignments for subpar reports via CVE request form - Chris Coffin and Jonathan Evans
Email thread on Board mailing list 10/23 - 11/13.
3:30 – 3:45: CVE communications, document repositories, and collaboration – Joe Sain
3:45 – 3:55: Open Discussion
3:55 – 4:00: Action items, wrap-up – Chris Coffin

Review of Action Items from Last Meeting

- **PREVIOUS ACTION ITEM:** Dave Waltermire volunteered to review current CNA rules for required items and flexible items.
    - **STATUS:** Dave emailed the Board on 11/14 and said he plans to complete the review soon
- **PREVIOUS ACTION ITEM:** MITRE will schedule a Board meeting that will include the representatives from GitHub.
    - **STATUS:** Kurt has met with GitHub and is already in discussions with them on being a CVE CNA. They are looking to be split into two CNAs, one for their own products and one for third-party code that they find vulnerabilities in as part of their normal operations. Kurt will work with the CVE team and the Board if there are questions or issues. Kurt stated: will likely be creating 2 CNAs, one for all products in Github, and one for their own products. Will need other CNAs to clearly mark their covered products on Github to avoid redundancy. Communication through the CNA list will help here.
- **PREVIOUS ACTION ITEM:** MITRE will start a discussion about additional technical domains and areas that should have CVE coverage.
    - **STATUS:** Has not been completed. MITRE will continue this as an action item for next call.
- **PREVIOUS ACTION ITEM:** The discussion on building the base (i.e., identifying and onboarding Root CNAs) will be discussed by the Strategic Planning WG.
    - **STATUS:** Strategic Planning WG document that can help start this conversation is in development. Some related discussions occurred in Strategic Planning WG meeting on 11/13.
- **PREVIOUS ACTION ITEM:** The discussion on broken links and handling them with the CVE downloads and JSON will continue in a Board email thread.
    - **STATUS:** Has not been completed. MITRE will continue this as an action item for next call. The discussion around handling broken links continues for the web site and some useful suggestions have been provided.
- **PREVIOUS ACTION ITEM:** Dave Waltermire will identify CVE quality issues and raise them with the Board.
    - **STATUS:** He will do this on an ongoing basis to highlight quality issues that affect downstream use of CVE information.

Agenda Items

Board Working Groups

Strategic Planning Working Group (Kent Landfield)

STATUS: Kent is currently assembling a document that captures recent conversations on strategy, questions that need to be answered, and what the ideas are on a path forward. He hopes to have it available within the next couple of weeks. Still some contention on bringing on Booz Allen Hamilton as a CNA in the researcher model. There is a desire for a bigger barrier to entry to the program, perhaps a 10 “good” CVE threshold, and a board interview? Also needs to ensure

that it doesn't become too difficult to join in. The Strategic Planning WG began discussions around CNA requirements in the 11/13 meeting and will continue this discussion in a later meeting.

ACTIONS: None

Automation Working Group (George Theall)

STATUS: Additional Ideas for phase 3 were discussed within the working group meeting on 11/13. Some automation goals for the pilot:

1) Automated validation of pull requests, (JSON is first, more to come)

2)automatic acceptance by policy (IBM is the first trusted CNA, their data will go straight through, CVSS from NIST as well)

3) Testing to determine how GitHub handles multiple updates from multiple sources occurring simultaneously (Heartbleed).

4) Management of disputes via GitHub issues.

ACTIONS: None

CNA Updates

DWF (Kurt Seifried)

STATUS: None

ISSUES/DISCUSSION: None

ACTIONS: None

MITRE (CVE Team)

STATUS: Booz Allen Hamilton and SAP were added as CNAs. SAP going public with advisories as of December.

DISCUSSION: Jonathan Evans, Nick Caron, and Joe Sain are going to be sharing CNA-related tasks going forward.

ACTIONS: None

Documentation: CNA Processes

STATUS/ISSUE: CNA Processes draft document has been made available for Board review. Board had until COB Dec. 1 to review and provide feedback.

DISCUSSION/NOTES: Kent strongly encouraged that the CVE team provide a separate email thread for document review moving forward. Threads on the board list would help, and would encourage more participation.

ACTIONS: CVE team was to provide the Board with a Board email thread and handshake announcement regarding the review task and attach the document.

Discussion: Problematic assignments for subpar reports via CVE request form

ISSUE: Problematic assignments for subpar reports Board email thread: we have an individual requesting a bunch of ids for a singular product that are questionable, (The individual in question is likely a person, university student in China)

DISCUSSION/NOTES:

We are trying to break down the problem into the more core or root issues.

Banning a requester: should we given that CVE is voluntary?

- Stack Overflow talk on communities/trolls. If we can't educate a provider, we should cut our losses. DWF bounces 1/3 of requests for being poor. Certain DWF requests are ignored based on history, (requests are maintained); this could be effectively considered banning.
- Historically, CVE hasn't banned anyone, de-prioritizing has happened based on refusal to improve the quality of submissions.
- Follow through on Kurt's idea of researcher review program? Star reviews?
- Kurt's methodology: cross-reference emails vs rejects, which provides an immediate dataset.
- Good requesters emerge as a positive history develops; this discourages email hopping.
- How do we represent quality to the community at large, and maintain transparency?
- As we make it easier to submit CVE requests, we need to provide a stick as well as a carrot; a rating system will ensure researchers still put in effort on their end.
- Is there an automated solution for this?
- One consideration: we need explicit separation of public/non-public info
- We can't do anything without a public data source though that is transparent

GitHub repository removal:

- All issues from this individual have been abandoned, their GitHub repository was cleaned out.
- Kurt: The expectation of privacy is gone, since this is post-publication
- We need to investigate if there is malicious intent; MITRE will ask the researcher why the GitHub repo was cleared out
- We could create our own repo, owned by CVE, could track orphaned information and act as provider.
- There are tools to grab pages, which could be used to capture content. We would need to account for issues like malware, but it should fall under fair use

- Another option could be for CVE to submit for archiving all references. This is problematic, however, as the submitter can opt out.
- It was also noted that a small set of CVEs dating back to early 1999 do not have references.
- How do we monitor CVEs without references? How to we ensure that these CVEs do get references in the future?
- How much formalization do we want for approaching bad requesters?

ACTIONS: Carry this discussion over to a Board email thread. MITRE will contact researcher to understand why the GitHub repository was cleared out.

CVE communications, document repositories, and collaboration

STATUS/ISSUE: Summary of current and future CVE communications, repositories, and collaboration options.

DISCUSSION/NOTES:

- There are currently many moving parts in communications, file hosting, and content development.
- MITRE is moving from LISTSERV to Microsoft groups, need to maintain compliance.
- This will result in some changes in way things work.
- The change will occur at end of December.
- Nabble email web archive currently hosts the public CVE Board mailing list. MITRE is investigating alternative offerings. (mail-archive, MarkMail, Hypermail)
- Document repositories to be organized as follows:
    - Final, approved documents will continue to reside on the CVE web site.
    - Documents that are staged for Board review and approval will reside on the CVE Board Handshake site.
    - Documents that are in the process of collaborative development and editing will reside on the CVE GitHub repository.
    - Notification of documents uploaded for editing, review and approval will be handled via the board list or via Handshake email, which is sent automatically upon upload.
- Handshake will be used for issue tracking and threaded discussions

ACTIONS: Some of the current issues and document reviews will be offered within Handshake to test it out and see if it meets the needs of the Board.

Summary of Action Items

- Kurt to work with GitHub on becoming a CNA
- Continue email discussions on Problematic assignments for subpar reports via CVE request form, banning requesters, references being removed
- Provide CNA processes doc via handshake and email

- Dave Waltermire volunteered to review current CNA rules for required items and flexible items.
- The CVE team will start a discussion about additional technical domains and areas that should have CVE coverage.
- The discussion on building the base (i.e., identifying and onboarding Root CNAs) will be discussed by the Strategic Planning WG.
- The discussion on broken links and handling them with the CVE downloads and JSON will continue in a Board email thread.

Significant Decisions:

None