CVE Board Meeting 29 November 2017

Board Members in Attendance

William Cox (Black Duck)
Kent Landfield (McAfee)
Scott Lawler (LP3)
Taki Uchiyama (JPCERT)
Dave Waltermire (NIST)

Members of MITRE CVE Team in Attendance

Jonathan Evans
Joe Sain
Anthony Singleton
George Theall
Alex Tweed

Agenda

2:00 – 2:05: Introductions, action items from the last meeting – Joe Sain
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
  - With sub CNAs forking DWFs repo some operational issues were found.
- Actions
  - Working to institute a branching approach to the current forking practices that will assist in keeping the repo clean with less problems.
- Board Decisions

General – Jonathan Evans, Nick Caron

- Issues
- Actions
- Board Decisions

2:50 – 2:55: CVE Board Handshake Site reminder – Joe Sain
2:55 – 3:00: Board Membership – Joe Sain
3:00 – 3:15: Broken References Discussion – George Theall
3:15 – 3:55: Open Discussion
3:55 – 4:00: Action items, wrap-up – Joe Sain

Action items from the last meeting

- Kurt to work with GitHub on becoming a CNA
  - Status: Kurt will work with GitHub to bring them on as a CNA. Kurt has talked with GitHub but a date for onboarding has not been set.
- Continue email discussions on problematic assignments for subpar reports via CVE request form, banning requesters, references being removed
  - Status: MITRE has not received any new emails from Carsten about the GitHub repo being cleared. MITRE did reach out to Lin regarding the repo. He did not provide a reason why it was cleared but did repopulate it with the original data.
- Provide CNA processes doc via handshake and email
  - Status: Completed. MITRE is looking for feedback on document by COB 12/4/17.
- Dave Waltermire volunteered to review current CNA rules for required items and flexible items.
  - Status: [IN MEETING UPDATE] Will provide all comments once his review is completed. Is looking to have it ready for 12/1 to review with the Strategic Planning Working Group.
- The CVE team will start a discussion about additional technical domains and areas that should have CVE coverage.
  - Status: In progress.
- The discussion on building the base (i.e., identifying and onboarding Root CNAs) will be discussed by the Strategic Planning WG.
  - Status: Today's meeting will discuss this. Refer to agenda item notes.
- Dave Waltermire will identify CVE quality issues and raise them with the Board.
  - Status: [IN MEETING UPDATE] Will continue efforts and will continue to communicate the issues found in entries.

Working Groups

Strategic Planning – Kent Landfield

- Issues
- Actions
  - Reviewing the CNA processing document
  - Looking to find a new meeting time that works for members of Group.
  - Meeting moved to 12/1
- Board Decisions
  - NONE

Automation – George Theall

- Issues

    - Kurt noted the importance of the use of branches in submitting CVE data.
    - Kurt is continuing to work on AWG tooling efforts.
- Actions
    - Wrapped up discussion on Phase 3 of GIT pilot.
    - AWG received rough draft of proposal
    - Looking to present to the board through mailing list next week.
- Board Decisions
    - NONE

CNA Update

DWF

- Issues
    - Sub CNAs forking DWF's repo is causing some operational issues.
- Actions
    - Working to institute a branching approach to the current forking practices that will assist in keep the repo clean with less problems.
- Board Decisions
    - NONE

General – Jonathan Evans, Nick Caron

- Issues
- Actions
    - Mostly have been handling issues with unresponsive CNAs, after review looks like technical difficulties and not CNAs ignoring requesters.
- Board Decisions
    - NONE

CVE Board Handshake Site reminder

- We will to continue to transition CVE Board collaboration functions to the Handshake platform. Some Board members have not completed the process of registering. Some invites have expired; new invites will be sent with instructions for completing the process.
- Testing with message thread will take place soon.

Board Membership

- Scott Moore has expressed interest to Join the CVE Board. Paperwork for nomination is in progress and will be sent to the private board list when completed.

Broken References Discussion

- There are two aspects for handling this
    - How data is Presented on CVE site = modify public website – make broken links un-clickable, use strike through and label as obsolete and then point back to archive if available.
    - In downloads, one option is to prefix reference source names; e.g., "obsolete-[sourcename]". Will need to provide downstream users that this may happen. A second is to add flags to sources stating that they are broken, this approach is more disruptive to downstream users.

    - The Board recommended creating documentation on how to properly parse and handle CVE data that can be fluid in its construction. A suggestion was made that this could be worked by the Automation WG.
    - Board believes proposal to make changes to the CVE MITRE site to be sent to the board list.
    - MITRE will look at the analytics on the usage of data feeds. Kent would like to see this information in 1 or 2 slides and be presented to the Board.
- MITRE provided details of possible domains types to support-
    - domains that are parked or have changed ownership (allaire.com / conectiva.com.br / immunix.org / ksrt.org)
    - domains that are still registered to the original owners but that fail to return anything (bindview.com / ftp.caldera.com / stage.caldera.com / iss.net / linux-mandrake.com / mandriva.com / milw0rm.com / vil.nai.com / ntbugtraq.com / sunsolve.sun.com / trustix.net / trustix.org)
    - domains that are still active but reference URLs are broken (atstake.com / bea.com / www.caldera.com / calderasystems.com / compaq.com / eeye.com / l0pht.com / macromedia.com / www.nai.com / osvdb.org / blogs.sun.com / bugs.sun.com / docs.sun.com / vupen.com)

Open Discussion

- Kent believes the Board charter should be revisited and a few items should be added. The charter states that reviews are yearly.

- Kent reminded MITRE that previous action items should be included in agendas for upcoming Board meetings.

- What is the status from the CVE Board mailing list participation responses. MITRE will review process for individuals who did not respond.

- Some organizations have approached MITRE to join effort for open source. MITRE has directed them to DWF. It is not clear what the responsibilities are for a Root. MITRE provides training for organizations. The Board would like to figure out whether the DWF can handle such operations and if not how can the Board and Program assist DWF in getting up to speed. Biggest issue will be coordination for DWF with organizations that would like to monitor a large scope of open source libraries, repos, etc.

    - David Waltermire believes a meeting with all parties involved to see where progress is and what can be done to get the DWF off the ground and running fully operationally. Possibly bring up the idea of instituting a multi-cna management structure for the DWF.

- Training Documents information is covered in the process document sent out to the board for review. MITRE currently has slide decks used in training new CNAs. The approach MITRE is taking is having the board review the process document for 2 weeks and in that time MITRE writes the next document.

- Discussion regarding CNA mailing list thread “How CVE-2015-7501 should be used” took place with not much of a solution of solid position being placed. MITRE explained their understanding and position to the issue in reference to the CNA rules.

- MITRE discusses Carsten’s original email thread by aligning his issues with the current process MITRE uses for assigning IDs for vulnerabilities. Board would like for MITRE to find the “happy medium” in quality of assignment and minimizing the amount of time it takes to assign IDs.

- Board asks about CNA summit and provides feedback on potential structure and ideas for what problems need to be solved and how to solve them.

Action items

- MITRE will send out note on handshake site for thread testing in email viewing.

- Strategic Planning Working Group will discuss CVE Processes and international participation

- MITRE will complete Scott Moore Board nomination and send it out.

- MITRE will look at data feed statistics and provide findings to the board.

- MITRE will set up meeting with DWF to discuss Linux distros hierarchy under DWF.

- MITRE will send out the slide deck used for CNA training.

- The Automation WG will look into documenting how downstream users should to handle CVE data downloads.

- MITRE will send proposal to board on how to handle broken links on the MITRE CVE site.