CVE Board Meeting 13 December 2017

Board Members in Attendance
William Cox (Black Duck)
Andy Balinsky (Cisco)
Beverly Finch (Lenovo)
Kent Landfield (McAfee)
Art Manion (CERT/CC)
Scott Moore (IBM)
Kurt Seifried (Red Hat/DWF)
Taki Uchiyama (JPCERT/CC)
Dave Waltermire (NIST)

Members of MITRE CVE Team in Attendance
Nick Caron
Chris Coffin
Christine Deal
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

- Issues
- Actions
- Board Decisions

2:50 - 3:00: CVE CNA Summit Planning – Joe Sain
3:00 – 3:30: Git Pilot Proposal for Phase 3 – George Theall

3:30 – 3:45: Documentation:
Charter Revisions - Chris Coffin, Kent Landfield
Process Document Revisions - Jonathan Evans
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:** MITRE will send out note on handshake site for thread testing in email viewing.
  - **STATUS:** In process; still onboarding Board members
- **PREVIOUS ACTION ITEM:** Strategy Planning group will discuss CVE Processes and international participation
  - **STATUS:** Complete; will be covered in Strategic Planning Working Group readout
- **PREVIOUS ACTION ITEM:** MITRE will complete Scott Moore Board nomination and send it out.
  - **STATUS:** Complete; Welcome, Scott!
- **PREVIOUS ACTION ITEM:** MITRE will look at data feed statistics and provide findings to the board.
  - **STATUS:** Assigned to Joe Sain; not yet started
- **PREVIOUS ACTION ITEM:** MITRE will set up meeting with DWF to discuss Linux distros hierarchy under DWF.
  - **STATUS:** That meeting is TBD
- **PREVIOUS ACTION ITEM:** MITRE will send out training slide decks used for training.
  - **STATUS:** The slide decks are being modified and will be ready for review in the next couple of weeks.
- **PREVIOUS ACTION ITEM:** AWG will look into documenting how downstream users should to handle CVE data downloads.
  - **STATUS:** This item has been tabled due to Git pilot but this item is next on the list.
- **PREVIOUS ACTION ITEM:** MITRE will send proposal to board on how to handle broken links on the MITRE CVE site.
  - **STATUS:** This has not yet been done but will be done soon.

Agenda Items

<u>Board Working Groups</u>

Strategic Planning Working Group (Kent Landfield)

STATUS: Spent quite a bit of the call on the CNA Processes document. Part of the discussion centered on making the document more general in nature, less specific to MITRE. Kent said the other major thing was that the Monday timeframe doesn't work for everyone. We need to figure out a better time and day to meet, maybe Tuesday or Thursday. A doodle poll has been requested, but hopefully we can narrow it to a couple of days to see what works best. Chris Coffin added that there was also discussion around block reservations and how that process works. Maybe we could do more on-demand type of reservations in the future, and do away with block assignments and unused IDs at the end of the year.

Dave Waltermire added that roles need to be better defined in the CNA Processes document but we can discuss that later since it's on the agenda.

ACTIONS: None

Automation Working Group (George Theall)

STATUS: Sent a note to the Board about phase 3 proposal. We went into more detail during Monday's meeting. Dave Waltermire was asking how we can handle automation of issue tracking. One of the things we came up with was using a set of JSON or XML files that CNAs could maintain and would indicate which GitHub usernames are are associated with a CNA, what their GPG keys are, what blocks they have if they choose to disclose that information, etc. We are going to draft up a schema and send to the Automation WG.

Kurt said Board should discuss whether blocks assignment information should be published for all CNAs.

Scott Moore added that IBM is working on signing requirement, which will take some work.

ACTIONS: None

<u>CNA Updates</u>

DWF (Kurt Seifried)

STATUS: Is developing best practices for working with Git and realizes the importance of protecting the "master" branch. He will then update the contributing document. Still trying to figure out the best way to update the pull requests where I'm not committing the branch to my master. On the CI front, came up with a list of basic checks before submission.

ISSUES/DISCUSSION: It would be nice to have vendors declare what their proper name is. Jonathan said it would be nice to have a registry where the CNAs register their name.

Dave Waltermire: From a product ID perspective, it would be great if a vendor marked whether their products were susceptible to a given vulnerability. Vendors would do a better job in a fraction of the time. Is there any way we can make more of that happen? For example, half of what the NVD does is, when they receive a vulnerability, they look through the prose description and it would be helpful to see which products are affected by that vulnerability. If we spend 15 minutes per vulnerability that comes in the door, 7-8 minutes are spent on the vulnerability configurations. Not always easy to come by.

Group consensus is that this is a problem that's bigger than CVE.

Art: The only scalable thing is something where like we are doing with CVE assignments and requests where the work is pushed back to the edges. If the upstream marks their product as vulnerable to x, that should flow down.

Dave: The job of vulnerability management gets easier as every new vendor starts to provide that work.

Art: There are some policy, political, technical aspects to it. I'm happy for CVE to participate or enable it to happen. But I'm throwing the scope flag, because it's not something we can easily do on the side while we're also doing CVE.

Kent: The Global Vulnerability Reporting Summit is happening in March in Osaka. Focus on getting advancements and large complex systems problems around vulnerability management.

Kurt: SWID tags. If we start collecting that information and publishing in a central and well-known location, it's not a waste of time. It will be useful.

Art and Kent: SWID tags are part of a potential solution.

Dave wrote a document about this in NISTIR 8060 and would like some feedback about what's missing.

Other documents mentioned during discussion include:

- https://scap.nist.gov/specifications/swid/
- https://www.congress.gov/bill/113th-congress/house-bill/5793

Dave W: We just want vendors to boil their portion of the ocean, not the entire ocean.

Chris C: What methods are being used right now to get vendors to boil their part of the ocean?

Dave: Three pronged-- 1) Focus on guidance (SWID tag guidance); 2) work around trying to develop tooling to support the adoption of SWID tags (published a SWID tag validator); 3) trying to talk to organizations about procurement requirements to get greater incentives out there.

ACTIONS: Kurt asked that Dave send out links to those standards documents via the email list. Kent--Encourage Board members to show up in Osaka. Dave, Kent, and Art to send email to CNA list with information we've discussed here.

MITRE (CVE Team)

STATUS: We've had a few organizations show some interest in becoming CNAs: BugCrowd, Hikvision (security camera producer in China), Sophos, FaceBook, and VMS/VSI (split off from HP). No new CNAs have been added, we are just in the beginning stages of talking to them.

DISCUSSION: None

ACTIONS: None

Canceling the Board meeting for December 27

No issues or discussion.

CVE CNA Summit Planning – Joe Sain

STATUS: Next CNA Summit is on February 13-14 on MITRE campus in McLean, VA. Working on logistics and starting to pull ideas for an agenda. It will be more of a working session this time, as opposed to a training session. We would like to hear from CNAs on issues/challenges; how to handle open source software and looking at root/subordinate CNAs and how that works in a federated environment. We welcome feedback from Board members. Will be sending out an email to the CNA list this week. Since it's on the MITRE campus, we have extra hoops to jump through regarding foreign nationals and countries of special interest, so we need to get a roster of attendees as soon as possible.

DISCUSSION: Might be nice to have a discussion on how best to obtain proper product names from vendors (SWID tags, etc.) at the CNA Summit. Art is willing to lead or guide a discussion on supply chain or inventory.

We got the most value out of open discussion during the last summit, so we'd like to have more of that format than a training session.

The Board would like to participate in creating the agenda.

ACTIONS: MITRE will get together initial thoughts on agenda and share with Board for feedback.

Git Pilot Proposal for Phase 3 – George Theall

STATUS: We are proposing to start phase 3 after this meeting and have it run through May. In Phase 1, we demonstrated the feasibility of using git to share assignment information. In Phase 2, we moved to a public repo on GitHub and phase 3 we will work on further workflow issues—

validation, automation, fixing broken links, updates to descriptions, etc. That's pretty much it. We'd like to open it up to all CNAs at top level (excluding sub-CNAs).

Types of validation: Signature checking—going up late today/early tomorrow. Checking for GPG signatures. Coming down pipeline: broken links, provenance checks on links (at least one reference that can corroborate that this entry should be completed). At the end of December—we are checking for ID ownership. Also in December, we will be auto processing requests for trusted CNAs. In January, making changes to an entry that you don't own. There will be a process for automating where the assigning CNA (that assigned the CVE id) will be automatically added to make sure that they can review any changes.

DISCUSSION: Will you be publishing infrastructure code (such as the validations) in a GitHub repo? Not at this time, but we can look into this and potentially begin publishing in the future. Can you publish the code even if you don't publish the database? Yes. This could be an option. Dave W: the more we continue to do that, the harder it becomes for us to shift gears and produce something that's public. At some point, we must commit to doing that and make the investment. How do we make forward progress on this issue? What's the next step? Can we create a Git repo on the project side called CVE validation so that we can add stuff there so that it's in an authoritative location? Chris adds that the data that is received has always been a closed source repository but we're slowly moving towards Git; we're maintaining both. Dave W: I understand that there are security challenges to address here, I know we've talked a lot about this but I don't see a lot of progress being made in that direction. The progress I've seen is around data and where it's published but I'd like to see progress around code. What can the Board do to ensure progress, and what are you doing in MITRE to ensure progress? Kurt: there might be value in breaking with the past. Maybe they should create the Git repo? Dave: there is a lot of work that needs to be done before we could do that—we'd have to re-invent the infrastructure.

ACTIONS: Dave will clarify via phone or email to explain exactly what specific code he is interested in seeing as a start. MITRE needs to set up another conversation to get this moving forward.

Documentation

Charter Revisions - Chris Coffin, Kent Landfield

STATUS/ISSUE: Had comments on charter. Updated version was sent out yesterday and is open for comments until December 22. Chris has some updates to the document based on an internal reviewer (i.e., CVE is used in different contexts throughout).

DISCUSSION/NOTES: This is a very specific document with MITRE as the Board Moderator, so it should not be made generic.

ACTIONS: Chris will send out another version (tomorrow or Friday) to incorporate recent edits. We need to update the website once the charter is revised.

CNA Process Document Revisions - Jonathan Evans

STATUS/ISSUE: We've been working on merging the version to adjudicate feedback from Board members; revisions mostly revolve around trying to make the document less specific to MITRE. There are a few issues that are more like CNA rule things that never got resolved-what the year and CVE ID mean and how you should use it to assign IDs. In the most recent revision of the rules, we say you must contact the parent CNA within 24 hours but that may be an issue if there is a chain of CNAs. New draft will be ready to go out tomorrow.

DISCUSSION/NOTES:

ACTIONS:

CNA Rules

DISCUSSION: Art: There is an issue that we need to talk about. The document was worked on and agree upon, posted to CNA list, that this is what we would use going forward. We don't want to jerk these guys around by constantly changing the rules. Art finally reviewed the document and notes there are some real problems from the standpoint it looks like it was developed by 12 people, uses inconsistent terminology, and explains things too simply. We need to make this look like a finished document as opposed to what it looks like now. It's not done in my opinion. Proposes the Board create a new version of the document (before the summit). We could even discuss at the summit. At this point, I'm under the assumption that I'm going to proceed that I'm going to edit the CNA rules document and then we can evaluate what the next steps are.

Chris: As long as we aren't changing processes, we can update several times a year.

ACTION: Art, Dave, and Kent are going to update the document and encourage other Board members to do so to hopefully have a revised version by February for the Summit. Kent has volunteered to be the editor.

Set up a discussion for the summit: Would be nice to get an understanding from the CNAs what are the risks we need to mitigate through the update process. What's the right way to manage those risks? What changes are most important for the CNAs?

<u>Open Discussion</u>

How do we conduct dispute resolution within CVE descriptions/CVSS? Kurt's preference is to strongly encourage convergence. He thinks in the short term, it would be good to allow other people to make claims, but what happens when we get a CVE that has two descriptions that are incompatible? It would be better, especially at the global level, to allow one statement and make it work. If an end user sees a CVE with two CVSS scores, on a global level, the user won't know which to believe.

Dave Waltermire said NVD only considers information that's publicly released. They are trying to encourage more disclosure.

Jonathan shared this: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0429

Kurt: we need to define a description at the root level (just one) and then we can allow additional descriptions at the vendor level.

George: We don't have those levels yet in CVE.

Is the answer convergence, or allowing trusted contributors to make as many additions as they want? May need to be a combination of the two.

Allow and encourage convergence and see what happens. Current version won't support this. We will have to wrap them into lists.

Containerize all the data—implications how you manage that data. Need additional discussions on pros/cons. Have a core CVE record and somewhere near the bottom we have containers item that is an array of different organizational containers that give the ability to have different metadata.

Do we want to give CNAs the option of adding authorization rules?

ACTION: Present to the Automation WG--Come up with a format

Kurt will start email about what we want to allow—behavior wise.

Summary of Action Items

- No board meeting on 12/27
- Encourage board members to attend Osaka
- Dave Waltermire will send out an email on SWID tags with links to standards documents. Kent Landfield and Art Manion will provide additional information.
- MITRE to add vendor and product naming discussion to CNA Summit agenda
- MITRE to send out draft CNA Summit agenda to the Board for feedback
- Dave to send email about infrastructure/code that should be shared with the community (GitHub discussion)
- MITRE to set up another call to discuss the infrastructure/code that should be shared with the community (GitHub issue)
- MITRE to send out new draft of Board charter
- MITRE to send out new draft of CNA processes document
- MITRE to set up CNA rules discussion at summit (What are the most impactful changes?)
- Art, Dave, and Kent to start on a CNA Rules document update (Kent will act as editor)
- Automation WG discussion needed on data authorizations
- Kent will send vulnerability discussion document that will be presented in Osaka

Significant Decisions:

None