CVE Board Meeting 21 March 2018

Board Members in Attendance

Andy Balinsky (Cisco)
William Cox (Black Duck Software)
Beverly Finch (Lenovo)
Chris Johnson (NIST)
Kent Landfield (McAfee)
Scott Moore (IBM)
Taki Uchiyama (JPCERT/CC)

Members of MITRE CVE Team in Attendance

Chris Coffin
Christine Deal
Jonathan Evans
Joe Sain
George Theall

Agenda

2:00 – 2:10: *Introductions, action items from the last meeting* – Chris Coffin

2:10 – 2:30: *Working Groups*

- Strategic Planning – Kent Landfield
- Automation – Chris Johnson, Chris Coffin

2:30 – 2:50: *CNA Update*

- DWF – Kurt Seifried
- JPCERT – Taki Uchiyama
- MITRE – Jonathan Evans, Nick Caron

2:50 – 3:20: *FIRST Technical Colloquium Osaka Readout* – Jonathan Evans, Kent Landfield, Art Manion, Dave Waltermire

3:20 – 3:50: *Open Discussion*

3:50 – 4:00: *Action items, wrap-up* – Chris Coffin

Review of Action Items from Last Meeting

- **Previous Action Item:** MITRE will set up a meeting with NIST to discuss Automation Working Group roles and responsibilities.

    - **Status:** Done.
- **Previous Action Item**: MITRE will begin rejecting invalid pull requests after 21 days
    - **Status**: On track.
- **Previous Action Item**: Automation WG to discuss new project groups and initiate that process.
    - **Status**: Process has been started.
- **Previous Action Item**: Strategic Planning WG to discuss rules of escalation above roots
    - **Status**: TBD
- **Previous Action Item**: Plan a Board discussion on CVE entry language requirements (English required?).
    - **Status**: We can discuss today if members wish.
- **Previous Action Item**: Plan a Board discussion on workflow for rejecting old pull requests
    - **Status**: We can discuss today if members wish.
- **Previous Action Item:** Updated Board charter with verbiage related to proxy voting
    - **Status:** Updated charter will be sent around today or tomorrow

Agenda Items

Board Working Groups

Strategic Planning Working Group (Kent Landfield)

ISSUES: Gave a readout of some of the things that occurred in Osaka. Also discussed how to deal with vendors who want more than they have proven they can handle. Consensus of WG is to get those who want to expand their scope to first prove they can deal with their own scope before allowing them to expand their scope.

ACTIONS: MITRE needs to write something up on scope to be added to the guidance or training material.

BOARD DECISIONS: None.

Automation Working Group (Chris Johnson / Chris Coffin)

ISSUES: Gave a brief overview of the draft charter that Chris Johnson put together. Sent out a note to the list to encourage people to review the draft charter (located on GitHub). Talked about projects we envision kicking off, particularly the CNA registry and JSON format projects. Orienting folks on what we are about to do. In follow up discussion, we talked about getting draft charters put together and GitHub repositories for each project. We also spent time talking about the agenda for the upcoming WG meeting and discussed roles/responsibilities. Discussed format of WG calls (roll call, actions, updates, etc.). Collaboration will be needed between/among projects.

ACTIONS: Working on draft charter, send invitation to folks on Automation WG list for first two projects (CNA registry and JSON format).

BOARD DECISIONS: None.

CNA Updates

DWF (Kurt Seifried)

STATUS: None.

ISSUES/DISCUSSION: None.

ACTIONS: None.

JPCERT (Taki Uchiyama)

STATUS: No updates this week.

ISSUES/DISCUSSION: None.

ACTIONS: None.

MITRE (CVE Team)

STATUS: Avaya and GitLab have both requested to become CNAs. We are going to start training SonicWall on Friday.

ISSUES/DISCUSSION: None.

ACTIONS: None.

FIRST Technical Colloquium Osaka Readout – (Jonathan Evans, Kent Landfield, Art Manion, Dave Waltermire)

DISCUSSION: Jonathan: Conference was about global vulnerability reporting. We had 7 topics we considered discussing—two topics of great interest were 1) software component identification and 2) vulnerability description format (more pertinent to CVE than software component ID). There was a lot of good discussion on what models there are, what models we need. It is clear that we don't understand all the use cases we might have for a vulnerability description format. I think the group generally considered using the VDO (NISTIR 8138) vulnerability description ontology as a vehicle to come up with something that would be unifying (but needs more work). The VDO is missing attack vectors and software components. NIST is preparing to start reviewing that and we will provide feedback on what changes should be made.

Chris: Anything that could apply to CVE?

Kent: No. That wasn't the intent of this effort. We did start off with voting on different topics we would like to discuss. We then were looking at what was needed by the community the most. There was a discussion on the Software Bill of Materials, which includes Software Identification Tags (SWID and Software Package data Exchange (SPDX). The group settled on SWID because it is an international standard that has wider scope and coverage than SPDX. NIST and others have the action to write a paper on Software Build of Materials using SWID. This paper will be integrated into the NIST IR that talks about SWID usage. The National Telecommunications and Information Administration (NTIA) is also working on putting together a Software Bill of Materials project, and we plan on taking the SWID document into that effort.

We combined vulnerability formats with automation, but we talked about them as if they were separate. The focus around a lot of this had to do with the Vulnerability Description Ontology (VDO). We talked about the proliferation of formats, how some of these formats could (initially developed for expediency or specific applications), provide value in going through the VDO. We need to create a reference format for the VDO that could be shared with threat intel communities, STIX, etc., to have a reference format that is beneficial for all. This could lead to the point where the VDO is what is exchanged, especially when rapid dissemination is important.

We talked about the need for the VDO to be updated; it has not been updated since the last CNA Summit in 2016. We talked about putting the information out in a GitHub repository, including the comments, so we could work on the VDO as a community. NIST has the action to set up this repository.

We were also shown a JPCERT effort to utilize and conceptualize the VDO. JPCERT has done an effort in this regard and there are some real useful description models they showed on the slides and they have notes of things that have been done and are working. One of the action items was Taki was going to translate those notes from Japanese to English and put in a GitHub. They created a VDO reference format. Their work has the potential to impact the vulnerability landscape in a positive way.

We did talk about automation, but much of the automation is focused on specific areas: vulnerability discovery, vulnerability reporting, vulnerability assessments, vulnerability identification, etc. These types of automation needs must be driven by use cases. We need to document the use cases for automation so that we drive the requirements as we go forward. There was a discussion about where we do this going forward. The first time that we met, Vulnerability Reporting and Data eXchange SIG (VRDX-SIG) was created. We may be using VRDX-SIG for future work going forward. Will be doing this (conference) again every two years—location will be different (won't always be in Japan).

Taki: JPCERT is trying to automate some of their coordination activities so they can store information in their systems using VDO, so that we can better automate sending vulnerability information to vendors, issuing CVSS scores, etc. As we try to do that, we analyzed the VDO—as an action item, we are going to send some of our comments of some things that need to be clarified in the VDO and I have some slides that I may be able to share (need approval to share) to show you better what we are trying to do at JPCERT.

ACTION: None.

Open Discussion

Joe: On February 19, an XKCD cartoon came out listing the "Leaked list of Major 2018 Security Vulnerabilities" (https://xkcd.com/1957/). The last line in the cartoon was "A flaw in MITRE's CVE database allows arbitrary code insertion." The next day, we found an Open Bug Bounty vulnerability notification (https://www.openbugbounty.org/reports/563906/), which identified a cross-site scripting issue. MITRE's Information Security contacted the researcher for more information, who indicated that it wasn't really a vulnerability, since the HTML is encapsulated. In addition, the issue only manifested itself in older browsers. We did patch the code that the researcher was attempting to abuse. The vulnerability was marked as "fixed," even though the issue was withdrawn by the researcher because it was not a vulnerability. Public disclosure of the finding was scheduled for release on March 22, 2018.

Discussion about rejecting old pull requests: We discussed rejecting them if they'd been out there for 21 days. We don't currently have any that have been outstanding for 21 days. If it becomes more of a problem, we can talk about automating the process.

Kent: In the previous agenda, there are two action items for me—can you please pull those forward so that I can be held accountable?

Summary of Action Items

- Kent Landfield to make minor addition to Board Charter Proxy Voting language and re-send to the Board
- Kent Landfield to write a message for the CNA list that describes the CNA Coordination Working Group
- 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.

Significant Decisions:

None.