The CVE Editorial Board met via teleconference on April 21, 2016. Members of the MITRE CVE Team also attended the call.

Board members in attendance were:

Andy Balinsky, Cisco
Harold Booth, NIST
Kent Landfield, Intel
Scott Lawler, LP3
Art Manion, CERT/CC
Pascal Meunier, CERIAS/Purdue University
Mike Prosser, Symantec
Kurt Seifried, Red Hat
Dave Waltermire, NIST
Ken Williams, CA Technologies

The first agenda item up for discussion was simplified counting tested through CNA pilots. A simplified counting document was sent to the Board list on March 28. The purpose of simplified counting is to streamline the counting of vulnerabilities and assigning CVE IDs to improve operations and efficiency and enable CNAs to follow the process. There could be a negative effect on quality; therefore, a test needs to be done before moving this into regular CVE production.

Simplified counting includes a claim-based model. CVE IDs will now be given in cases where a researcher finds a flaw or design oversight in software, even though it may not be seen as a vulnerability by the vendor. The researcher may be asked to provide evidence of a demonstrated negative impact, such as an example/scenario where the flaw is exploitable.

CVE will be bringing Intel on as a CNA. The simplified counting document could be used as part of the training process with Intel. The nature and size of the vulnerabilities coming out of Intel will allow the CVE Team to see what works and what doesn't work in a standard test environment. A call will be set up with Intel's Product Security Incident Response Team (PSIRT) contacts to explain this to them and ensure they fully understand, making for a smoother test.

The discussion turned to the second agenda item, the DWF CNA Proposal. The proposal is to allow the DWF CNA to create and train subordinate CNAs. DWF and the sub-CNAs it creates will use the current counting criteria to assign CVE IDs. The sub-CNAs will operate within DWF's allocated CVE ID block. The sub-CNAs will need to be educated by DWF about the infrastructure, scope, etc. Terminology and documentation need to be established, as do the hierarchy and the processes in the hierarchy. Downstream impacts will be assessed. The goal is to scale CVE, get more CVEs out faster, and determine the validity of the federated model.

DWF operates with real-time transparency via GitHub. DWF has a simple database for entries. DWF requires researchers to provide an artifact as proof of a vulnerability, such as the source

code and research, before entries are put into the DWF database. The artifacts and other well-defined information are maintained in another database. All DWF data is Apache-licensed. MITRE will need to consult with their Legal Department about allowing for broad, distributed writing in the CVE corpus and using the Apache license to pull in data, and potential IPR issues. The plan is to get the CNA process moving forward for DWF next week to make it official.

A public list of officially recognized CNAs is available and will be maintained on the CVE website to direct CVE ID request submissions. A private list of individual's contact information will also be maintained for CNA relationship management and the communities being served. Documentation will be created in two phases:
Phase 1: DWF as a classic CNA
Phase 2: Sub-CNA hierarchy and rules

Qualitative measurements matter most right now, both to MITRE and the community. MITRE needs a better sense of broader CVE operations beyond the DWF CNA. Qualitative measurements will be considered, such as if complaints decrease, the CVEs produced by the DWF CNA are working downstream, or whether people are seeking alternatives to CVE. Quantitative measurements are also possible: monitor metrics provided by GitHub, count how many IDs are assigned, and identify mean response times to assignment requests. Progress will be discussed via Editorial Board calls every other week.

The CVE Editorial Board E-mail Lists were then discussed, focusing on the private Editorial Board email list. The intent of the private list is that, if someone posts to the private list, that email remains private. There are occasions where the Board needs to have private conversations (e.g., new Board members, the ID syntax change).

The decision was made to retain the private list and to maintain its original intent. When an email is posted to the private list, it should include a reason why the email is being posted to the private list in the message to help eliminate confusion. If a Board member feels a topic needs to be moved to the public Editorial Board email list, the courtesy of asking the other Board members will be given.

Action items:

- Investigate IPR with MITRE legal (MITRE)
- Identify reasonable guideline for others, Apache or other acceptable license for generic usage of CVEs and content (MITRE and DWF)
- Stand up Phase 1 DWF CNA next week (MITRE and DWF)
- Set up Intel PSIRT coordination call for CVE issuance, the counting experiment (MITRE)
- Identify a set of documents MITRE would like to give to new CNAs (title plus a one sentence abstract) (MITRE)
- Reconcile MITRE/DWF documents (MITRE and DWF)
- Look into implications of CVE ID block; set up integration working session (MITRE)
- Study to move CVEs read/only on github.com (MITRE)

The next Editorial Board meeting will be held on May 5, 2016.