CVE Board Meeting
28 July 2016

The CVE Board met via teleconference on 28 July 2016. The meeting included updates on Distributed Weakness Filing (DWF) activities, the CVE Counting Rules document, the Board charter revisions, and the CVE Terms of Use (TOU). Members of the MITRE CVE Team also attended the call. Board members in attendance were:

Attendees:
Art Manion, CERT
Kurt Seifried, Red Hat
Harold Booth, NIST
Mark Cox, Red Hat
Pascal Meunier, CERIAS/Purdue University
Ken Williams, CA Technologies
Scott Lawler, LP3

Action items from the previous Board meeting were reviewed:

- Board Charter (MITRE)
    - Feedback from last meeting was incorporated into the document
    - Voting was postponed for the Charter due to outstanding issues brought up in the mailing list discussion
    - Tally from previous vote was distributed to Board mailing list
- CVE Counting Rules (MITRE)
    - Incorporated comments from feedback received

The meeting began with a DWF update. DWF has been assigning CVE IDs and they are starting the training process. The Board Moderator asked DWF to provide some metrics (e.g., how much time—approximately—is spent on training and what impact that had them) so that, going forward, that information is available as new root CNAs are established.

DWF has experienced a nuisance level of spam—not necessarily malicious, but poorly formatted requests (or requests that might be for a legitimate security hardening issue, but not a vulnerability). So far, they have received about 100 such requests, which is roughly a 5-10% spam rate.

The discussion then turned to the counting rules document. The new version of the counting rules document is ready, along with a new document concerning counting decisions for CNAs (i.e., the decision trees). MITRE is looking for feedback from everyone on the decision tree overall; feedback can be given via email. MITRE wants to know, specifically:

- Is it a step in the right direction?
- Are we simplifying things based on the earlier counting decisions?

- Are we missing anything major?
- Should we allow this kind of flexibility (the currently proposed decision tree allows for quite a bit of flexibility in the way CNAs would be able to count)?

The next step is to lock down the definition of what the "independently fixable" rule is; there is some room for interpretation.

There was some back and forth about the idea that, if only the vendor of a product can take an action to fix the vulnerability, perhaps a CVE ID should not be assigned. A concern was voiced that, if, for example, a Software as a Service (SaaS) product is vulnerable temporarily, there are no artifacts. So, how is that tracked, and how do we get these vendors onboard? What's their incentive to bare all? In that case, some type of identifier is needed for these types of issues, but at least one Board member said they are not sure that CVE is the right place to do that. It was generally agreed that CVE could be used as a core element in a domain-custom vulnerability management process where these things could be named in a way that is unique to their environment (domain), but still work with the broader CVE corpus.

The Board discussed the Charter next. While the Charter was initially out for a vote after the last meeting, outstanding issues brought up in the mailing list discussion prompted a postponement of the vote. Instead, a list of these outstanding issues was discussed via the private e-mail and during the Board meeting. The following is a list of the issues, and options for each issue, that will be put out for a Board vote prior to being incorporated into the Charter:

- Who makes the decision to award Emeritus status?
  - The Board Moderator
  - The Board, through a Board vote
  - The Board Moderator, but the Board can overrule the decision with a Board vote
- How much time should be provided to Board members to vote on a given issue?
  - One week
  - Two weeks
  - Time frames in which to cast a vote may vary as circumstances require, but must be at least one-week long. Two weeks is the recommended time frame for most votes, but is not required.
- Do you support adding the statements below to the Charter?
  Board members have a responsibility to participate by voting. Members will lose voting privileges if they do not vote in at least one of the three previous (consecutive) Board votes. Votes to abstain count toward participation and toward a quorum. Members may regain voting privileges by asking to have their voting privileges reinstated through the private mailing list or during a Board meeting. If Members have not voted in the past year, they can be removed from the Board by Board vote, following the procedures for forced removal.
  - Yes

- No

Last on the agenda was an update on the TOU document. Red Hat's lawyers (on behalf of DWF) have been reviewing the TOU so, to be fair, the opportunity was presented for other organizations to have their lawyers also review and comment on the TOU. So far, there have been no responses. A deadline of 8/5 was set for any organization to express an intent for their lawyers to contact MITRE's lawyers regarding the TOU.

Action items:

1. DWF—look toward getting some statistics with regard to training and overhead
2. CNA counting document (counting decision tree)—Expecting feedback by COB 8/8
3. Charter—call to vote for outstanding issues will go out 7/29.
4. Terms of Use—A solicitation will be sent to the list for organizations to express intent to have their lawyers contact MITRE's lawyers by 8/5 if there is a need.

The next Board meeting will be held on August 11.