CVE Editorial Board Meeting
30 June 2016, 2:00 p.m. EST

The CVE Editorial Board met via teleconference on 30 June 2016. The meeting was focused on Charter revisions and CVE counting rules. Members of the MITRE CVE Team also attended the call. Board members in attendance were:

Attendees:
Kent Landfield, Intel
Harold Booth, NIST
Andy Balinsky, Cisco
Scott Lawler, LP3
Art Manion, CERT
Dave Waltermire, NIST

Action items from the previous Editorial Board meeting were reviewed:
Action items:

- Board Charter (MITRE)
    - The revised Editorial Board Charter was distributed and discussed in this meeting
- Template for Board nominations (MITRE)
    - A proposed nomination form is now in Appendix A of the Charter
- Write a draft of CNA requirements based on what was discussed
    - CERT-CC will review CNA requirements document
- Update the CERT-CC swim lane description
    - An update to the CERT-CC Swim Lane description is nearly completed and will be distributed soon

There was a brief discussion concerning the current status of the CVE Terms of Use. Lawyers from RedHat, representing DWF voluntarily and not as RedHat, are working with MITRE's lawyers to finalize the updates. The Board members on the call requested that they, too, be able to review the Terms of Use before they are made public. MITRE agreed.

The conversation turned to the Editorial Board Charter, which had been distributed for review and comment for the previous two weeks. Revisions that did not change meaning or procedure were incorporated. Several suggested edits, however, would change meaning or procedure and so require a Board vote. These items were reviewed so that opinions could be heard and alternatives raised. Following are the items to be voted on, the alternatives, and the rationale for those alternatives:

1. **Should the name of the Board be:**
    a. **CVE Editorial Board** – This is the traditional name of the Board, and so requires no changes. However, this name was used because, when CVE was founded, the Board edited individual CVEs, which is no longer the case.

b. **CVE Advisory Board** – This name was proposed as aligning more closely with the current role of the Board, however, it will require adjustments to language (e.g., website updates).
c. **CVE Board** – This name was proposed as the most flexible alternative, though some found it to be so generic as to imply the Board controls all aspects of CVEs.

2. **Should Charter sections 1.3.1 through 1.3.4, listing specific tasks and qualifications for each Board Member role, be removed?**
    a. **Yes** – Removing these sections removes burdensome and unenforceable requirements and opens up participation. However, removing these also removes potential criteria against which Board nominations may be evaluated.
    b. **No** – Leaving these sections provides clear criteria for reviewing Board nominations. However, the strict language may make it difficult to accept nominees who would bring value to the CVE program but may not match all criteria.

3. **Should a 2/3 vote be required for forced removal, rather than simple majority?**
    a. **Yes** – A more stringent requirement than simple majority will reduce the chances of an individual being removed simply due to unpopular opinion. However, this does create a single case where a vote requires more than a majority decision.
    b. **No** – A majority vote ensures consistency across voting practices. However, it may make it too easy to forcibly remove someone who may bring value to the Board.

4. **For members of the Board to create a working group:**
    a. **No approval is needed.** – This option eliminates obstacles to quick action. However, it is possible that a few Board Members may form a working group under the auspices of the CVE Editorial Board that undermines the CVE program.
    b. **The Board Moderator provides approval. The Board may call a vote if it deems necessary, the results of which would determine approval.** – This option allows a fairly quick response while still ensuring there is a system of checks-and-balances. However, it is slower than forming a group without approval and could potentially be much slower if the Board decides a vote is needed.
    c. **A Board vote is required.** – This ensures the Board members all have a say in the formation of working groups. However, this method requires a waiting period while a vote is released, responded to, and counted.

A voting form is to be distributed along with the draft meeting minutes and summary on July 5 or 6. Votes must be in no later than July 13 so an updated charter can be ready for review by the next Editorial Board meeting on July 14. After the meeting on July 14, there will be a vote to accept the revised Charter.

Changes to the Counting Paper were then discussed. Feedback was collected from Board Members prior to the meeting, and some changes were discussed in detail:

1. Currently, MITRE holds off on counting an issue as a vulnerability until we have confirmed with a vendor that it is in violation of their security policy. The proposed change is that this moves to a claims-based model. If there is a demonstrated impact, but it's not clear if it violates the security policy, an ID will be assigned. – Board members agreed with this change, provided it is possible to reject if later found not to be in violation of the vendor's security policy.

2. Currently, when MITRE gets a request for unfamiliar product, time is spent determining if that product is installable in the customer environment. The proposed change is, when it is not clear, an ID will be assigned. – – Board members agreed with this change, provided it is possible to reject if later found not to be an installable product. Also, at least one board member feels that Software-as-a-Service vulnerabilities should be included within the scope and coverage of the CVE program.

3. Currently, when a request is received for something that's potentially a shared code base vulnerability, MITRE researches to determine whether it is or not. The proposed change is to not do that additional research and go ahead and assign to every product that is affected regardless of shared code base. However, if it is called out that it's a shared code base issue, it will be treated as such. – Board members agreed with this change, provided it is possible to correct the situation later. There needs to be a review and documentation of the clean-up procedure, because downstream users will have to deal with this.

Currently, a separate CVE ID is created for separate types of vulnerabilities (e.g., multiple buffer overflows in same version of the product would be merged using the current process). The proposed change is to base counting on independently fixable issues. In the example above, if those buffer overflows can be fixed independently, then each buffer overflow vulnerability would be assigned a separate CVE ID. – Board members generally agreed, but concerns were raised such as an expectation that counting would be wrong on a consistent basis due to lack of understanding or misinterpretation of the counting rules.
Action items:

- Distribute a voting form for the outstanding Charter issues (MITRE)
- Incorporate the results of the vote and send out a revised Charter (MITRE)
- Incorporate comments received on the Counting Rules document and distribute it for final approval (MITRE)

Outstanding Action Items:

- Update the CERT-CC Swim Lane description (CERT-CC; in progress)
- Revise the CNA requirements document (CERT-CC)

The next Editorial Board meeting will be held on July 14.