The Editorial Board (EB) met via teleconference on 30 March 2016 from 13:00 to 17:00 EDT. In addition to members of the MITRE CVE Team, the following individuals attended the call.

- Kent Landfield, Intel
- Scott Lawler, LP3
- David Waltermire, NIST
- Harold Booth, NIST
- Mark-David McLaughlin, Cisco
- Pascal Meunier, Purdue
- Ken Williams, CA Technologies
- Kurt Seifried, RedHat
- Mark Cox, RedHat
- Art Manion, CERT/CC
- Tom Millar, US Department of Homeland Security (DHS)

The EB agreed that the processes being used currently to support the CVE project are outdated and not sufficient for the current or future state of vulnerability management. There is a perception that the project has been too slow to respond or adapt to the evolving set of stakeholder needs such as vulnerability researchers, who are a constantly-growing source of CVE ID requests.

The EB considers there to be two categories of issues that need to be addressed. There are short-term issues that relate to the current state of CVE and its problems. There are also long-term issues that are related to the vision of what CVE will be in the far future and how it will grow and evolve to meet the needs of stakeholders five or more years in the future. Though there are very specific problems that need addressing today, any changes to CVE processes or policy should take the vision of CVE in the future into account. Therefore, that vision will need to be defined as soon as possible.

The EB also agreed that the balance between the quality of information associated with CVE IDs and the speed at which those IDs are assigned needs to be reevaluated. Until recently, the CVE Team has attempted to maintain a very high standard with regard to the accuracy and completeness of information published within CVE entries, but this has resulted in a backlog of CVE ID requests, assignment, and publications.

A number of EB members suggested that CVE should shift toward a “fail-fast” paradigm. Currently, changes to the CVE process happen over time, during which the problems that those changes hope to resolve continue to hamper CVE stakeholder work. By accepting that mistakes will be made and creating processes that can quickly and cheaply correct those mistakes, CVE can evolve and adapt more quickly to the changing world.

Another significant point of discussion was the idea that CVE Numbering Authorities (CNAs) could play a bigger role in CVE assignment and management. Currently, the MITRE CVE Team

shoulders a significant part of the CVE assignment process, and cannot accommodate the growing number of CVE assignment requests and related work to the level that is needed by the stakeholders. CNAs could share that burden by taking on additional tasks in the CVE assignment process. The EB plans to explore what additional roles and tasks CNAs could take on going forward. Also, the EB would like to evaluate the process for adding new CNAs to determine how more CNAs could be included in the CVE process.

Before that work can take place, though, the EB realized that there are other issues that should be resolved first. Specifically, the EB will document all current and projected use cases, which will inform the EB as to what levels of quality are expected from CVE entries. Once quality is defined, the specific rules for CVE counting (how to determine the correct number of CVE IDs to apply to a vulnerability disclosure) can be redefined. With all this documented, the requirements for CNA operations can be codified. With the CNA role codified, CVE can work to expand the CVE project through federation with other CVE-like entities or with CNAs, which may increase in number.

As part of the "fail-fast" concept, the EB discussed the value of creating experimental, sanctioned projects related to CVE. One example of this is the DWF vulnerability numbering system. The EB will look at how DWF could be integrated with the formal CVE process such that CVE can better understand the specific set of use cases that DWF (Distributed Weakness Filing) was designed to satisfy. Going forward, other experimental projects could be developed in concert with the CVE Team and the EB, and the EB will look for other opportunities for such experimentation.

MITRE has attempted to maintain transparency into their processes, but the methodologies and processes used for sharing information have not been effective. The EB and MITRE agreed to create a github space to store public CVE documentation and allow for the EB and other stakeholders to collaborate on their development and improvement.

One example of this documentation work is the CVE charter, which will be revised in a number of ways. The role of DHS will be more formally documented, as will the role of the EB and other processes.

The EB felt that a face-to-face meeting would be useful for working through many of these issues. Once some additional groundwork and research is done by the EB and MITRE, such a meeting will be scheduled with remote participation as an option.

Action items

- MITRE will create a github site for CVE documentation.
    - A message will go out to the Editorial Board when the site is available.
- The EB will work with DWF to determine how best to integration DWF with CVE. They will look at documents describing well-formed CVE requests from both DWF and MITRE and will offer a comparison to inform the process.
- MITRE will schedule EB meetings to be held once every two weeks.

- MITRE and DHS will propose:
    - A DHS delegate will be an official member of the Editorial Board.
    - The CVE charter will be restructured and rewritten to address a number of issues.
- Mark-David McLaughlin took an action on behalf of Cisco to provide the names of the two Cisco CVE Editorial Board Members. Cisco's acquisition of Lancope means that there are currently three Cisco representatives, Andy Balinsky, Tim Keanini, and the departing Panos Kampanakis. Mr. McLaughlin had been nominated to replace Mr. Kampanakis.
- The EB will collect use cases from EB members, including the MITRE CVE Team, and present a summary of those use cases at an upcoming meeting.
- MITRE will investigate and present on models of existing federated identification schemes, such as ISBN.