OVAL Board Meeting (4/28/2014)

Attendees

Jamie Cromer – Symantec Corporation
Blake Frantz – Center for Internet Security
Tigran Gevorgyan – Qualys, Inc.
Steve Grubb – Red Hat Inc.
Morey Haber – BeyondTrust, Inc.
Kent Landfield – McAfee, Inc.
Dennis Moreau – VMware
William Munyan – Center for Internet Security
Steven Piliero – Unified Compliance
Dale Rich – DTCC
Amaresh Shirsat – Symantec Corporation
David Solin – jOVAL.org
Randy Taylor – ThreatGuard, Inc.
Jack Vander Pol – SPAWAR, U.S. Navy
Dave Waltermire – NIST
Chris Wood – Assuria Limited

Jonathan Baker – MITRE
Matt Hansbury – MITRE
Danny Haynes – MITRE
Luis Nunez – MITRE
David Rothenberg – MITRE

Invited Guests

Kim Watson – DHS

Meeting Summary

Welcome

The group was welcomed to the follow-up call for the 2014 2nd quarter OVAL Board Meeting.

Status Report

A status update of the OVAL project was delivered. The following items were covered:

OVAL Language/Interpreter

MITRE began by presenting recent updates to the OVAL Language. The OVAL Board has voted upon and approved the systemmetric_test and ntuser_test for the OVAL 5.11 release. Although this test was included in a previous voting and discussion period, MITRE has re-opened a two-week discussion period on the Windows license_test given the open questions on it.

Additionally, Cisco has been actively updating their OVAL Sandbox schemas. Their goal is to introduce tests that cover the assessment of the Cisco ASA, IOS, and IOS-XE platforms into the OVAL 5.11 release.

They have planned a community discussion to be held on May 5th to discuss the impacts of deprecating the existing PIXOS and CatOS platforms in favor of the two new platforms as well as address questions that have been raised by the community.

Lastly, Version 5.10.1.7 of the OVAL Interpreter was released on April 10th. This update fixed an error introduced in the previous Interpreter release for the importing of OVAL Directives and OVAL Definition evaluation-id files. Additionally, MITRE has added support for 64-bit RPMs and will be providing these through SourceForge in addition to previously offered download bundles. Also included were numerous bug fixes requested by the community.

OVAL Repository

At the time of the call, the number of Definitions within the OVAL Repository was 22,306. The OVAL Repository Top Contributor awards were presented to ALTX-SOFT, Hewlett-Packard, and SecPod Technologies for their numerous contributions.

Additionally, MITRE brought an issue with some of the OVAL Repository Definitions to the Board's attention. Historically, patch Definitions in the Repository did not include CVE references; however a number of recent contributions included references for each CVE covered by the relevant patch. This new usage exercised a bug in the code that sync's the OVAL description for a Definition with that found for a given CVE. The code incorrectly applied this logic to 'patch' Definitions in addition to 'vulnerability' Definitions. The bug has been fixed.

As a result, just over 2000 Definitions now have incorrect descriptions. MITRE has posed several possible solutions to the oval-discussion-list, and any Board members with thoughts on the subject were asked to respond to that email with their ideas.

OVAL Adoption

Official OVAL Adopters

- Center for Internet Security for their CIS-CAT product
- SPAWAR for their SCAP Compliance Checker (SCC) product
- Altex-Soft for their RedCheck product
- SecPod for their Saner product

Declarations

- Agiliance for their RiskVision product
- ADTsys for their ADTsys Cloud Security product
- SUSE for their SUSE Manager product

Unofficial Extensions in OVAL

MITRE introduced the topic of how to approach unofficial extensions within OVAL. The OVAL Sandbox addressed a long-time need to have a place to share and develop new and/or experimental Schemas and tests. With the new direction of OVAL, MITRE will reduce their level of moderation of the Language in order to better support the sponsor. With the change, it is imperative that the OVAL Board and

community continue to embrace a more critical role with OVAL. The issue in question is what to do with contributions to the Sandbox which may not be appropriate to bring into the official OVAL Language, yet still offer value. In an environment with less moderation, this may be tougher to coordinate.

MITRE has defined for these purposes that an "unofficial extension" to OVAL is one or more constructs that are considered ready for use and supports specific capabilities, while not being officially incorporated into the Language. It is important to note that currently, contributions to the OVAL Sandbox should not always be considered unofficial extensions. As those features mature, they may be voted upon for inclusion in an official release. However, there is the potential that under the new security automation vision, all future extensions to the Language will be considered unofficial.

A discussion on the merits of documenting unofficial extension support was opened to the OVAL Board. One Board member was concerned that by documenting how to support unofficial extensions, we were effectively making them official. This member voiced his opinion that any subscriber to the OVAL Developer List may craft an unofficial extension, support it in their product, and share it. This action shouldn't require a process but rather an understanding and delineation between that extension and what is official. As a tool vendor, they do not add capabilities to their product based on the construct being designated as "official," but rather based off the needs of their customers. He adds that it is not a minor effort to add a new Test and views the real benefit as simply staying ahead of the next version of the Language. He views this as more of a self-organizing problem and not a discussion for the Board. At this point, the DHS sponsor noted that if the community was unable to self-organize then they would have to pay someone to manage it. It would be ideal if the community had documentation for how to best approach supporting extensions without the need of a moderator.

Another member also urged the Board to consider improved documentation for how to extend the Language. Since everyone is free to update their own products then they should not be encumbered by waiting for a glacial process. Several members agreed that nothing is stopping people from doing this today, but, it would better help those hosting content to begin supporting unofficial content. This documentation could be achieved through a simple wiki page linked to by the Sandbox, showing how to conform to standard schema design. MITRE confirmed that this documentation was not required to be extensive and that the previous discussion supported this idea.

The approach of using unofficial extensions in OVAL was then compared to existing protocols in a standards body. A Board member noted that something like SNMP has a core schema, and that the bulk is managed through proprietary extensions. Providing guidance on how to extend OVAL is the type of documentation that is required in order to transition parts of OVAL to an international standards body.

Another point of emphasis among members was that it is essential that what is considered Core features of OVAL be documented and cleanly separated from extensions. There was not an immediate agreement on how to do this within the current OVAL release. Since all platforms relied on the core schemas they could be viewed as extensions. OVAL functions in general could also be redesigned to include the "core" functions and support platform-specific functions. The enumeration of datatypes was also examined and noted that not all existing datatypes are applicable to all platforms. Some vendors

may also wish to define their own datatypes. It was generally agreed that more thought needs to occur with respect to the separation of the Core features from extensions.

MITRE made the observation that there may be two approaches necessary to cover short term and long term goals. Upon finishing the OVAL 5.11 release, MITRE must begin focusing on supporting the US Government's security automation strategy and vision. They questioned how to support unofficial extensions in the gap between those two since some unofficial functionality may be needed. One Board member noted that the average SCAP revision cycle has been between 5 and 6 years. It needs to be decided what to do during the transition period, with the hope to relegate new platform extensions to primary source vendors. Another member added that the official Language is mainly comprised of consistent and agreed upon capabilities. If the change was made to only support the "core" and other consistent platforms then there would not be a need for a post-OVAL 5.11 release. The OVAL community would need to give consensus to capabilities in the Sandbox. Several Board members agreed that at this point, documentation for how this can be accomplished should suffice.

One idea suggested was to remove the demarcation of "official" and "unofficial" since they only pertained to SCAP Validation. If the perception of what is acceptable to use within a tool sold to the US Government could change, then the Language would be more flexible as a checking engine. Regardless of how OVAL decides to determine 'official' vs. 'unofficial' from here on, there is a hard box around what may be sold to the US Government for at least two years. This planned documentation should include references on how to interface with the existing Language, which would allow for better scanning in the gaps between releases. Another OVAL Board member also suggested that they like the tiered approach that NIST uses for SCAP content and maybe a similar approach could be used for classifying OVAL extensions.

Conclusion

MITRE has identified the need to determine what the "core" of the OVAL Language includes. This will be combined with previous discussions about a separate versioning policy for platforms to achieve higher stability by reducing unnecessary revisions. There is also a need to draft documentation outlining how the community may find, develop, and support extensions to OVAL. MITRE, with the OVAL Board, will continue to reduce the reliance on the need for a moderator in various activities related to the OVAL project.

Action Items

1. MITRE to determine distinction between core and platform extensions
2. MITRE to further develop the proposal for a separate versioning policy
3. MITRE to document best practices for extending the OVAL Language