

OVAL Board Meeting (07/08/2013)

Attendees

Scott Armstrong – Symantec Corporation
Anthony Busciglio – Cisco Systems, Inc.
Aharon Chernin – DTCC
Steve Grubb – Red Hat Inc.
Kent Landfield – McAfee, Inc.
William Munyan – Center for Internet Security
Omar Santos – Cisco Systems, Inc.
Randy Taylor – ThreatGuard, Inc.
Eric Walker – IBM Corp.
Dave Waltermire – NIST

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

Meeting Summary

Welcome

The group was welcomed to the 2013 3rd quarter OVAL Board Meeting.

Status Report

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

OVAL Adoption

Official OVAL Adopters

- Information-technology Promotion Agency in Japan for their My JVN API
- GCP Global for their ORCA product
- NopSec, Inc. for their Unified Vulnerability Risk Management product

OVAL Repository

A significant milestone has been achieved for the OVAL Repository. The Repository has passed 15,000 Definitions, with the exact total at the time of the call being 15,233 Definitions. The past quarter's top contributors were ALTX-SOFT, G2, Inc. and SecPod Technologies.

OVAL Interpreter

The OVAL Team released version 5.10.1.5 of the Interpreter on April 17th. Significant changes include adding support for the `ipv6_address` datatype, improving how the `signature_keyid` entity is collected in the `linux-sc:rpminfo_item`, and updating the collection of the `language` entity in the `win-sc:file_item` to better match the native format specified by the OS. This release also includes several bug fixes.

OVAL Language

Most of the Language work performed this last quarter has been in preparation for OVAL 5.11. This includes holding a conference call on May 6th to discuss the ongoing OVAL and Android work being done in the OVAL Sandbox. This talk examined the updated schemas and announced MITRE's Android System Characteristics generator tool, which can now be found in the OVAL Sandbox. The OVAL Team has also been working with Oracle to develop extensions to support the new features in Solaris 11. Lastly, much work has been done in preparing for the Developer Days event coming up in July.

Developer Days Overview

An update for the upcoming Developer Days event was provided to the OVAL Board. At the time of the call, the number of registered attendees was up to 84 persons. Registration has officially closed, but with several spots available, registrations could still be granted. A draft of the agenda has been posted on the registration page, with a planned finalized agenda to go out the following week. It was discussed that the reason for moving the location to the Washington DC region this year was to allow participation from those with travel restrictions in the DC area.

The general topics for the Developer Days event will be split over the three days. Remediation topics will be the main focus for Monday morning. This is followed by OVAL topics on Monday afternoon as well as all of Tuesday. Scheduled talks for OVAL include a discussion of the Sandbox process and how its gaps could be improved, a celebration of the 10th anniversary of OVAL, and many Language issues targeted towards the OVAL 5.11 release. On Tuesday evening, a social event will be held at Gordon Biersch in the nearby Tysons Corner mall. The bulk of Wednesday's talks will be led by Joe Wolfkiel, discussing the CMRS project and its effect on tool vendors.

Discussion

The main question relating to the Developer Days discussion was whether or not there would be planned technical presentations. The MITRE Team clarified that there would be a number of technical presentations this year, in large part from presenters that would like to introduce one or more OVAL Sandbox changes to the community and work towards getting them into the next version of the OVAL Language. A follow-up question was whether there would be any read-ahead materials provided prior to the event. There will be read-ahead materials that should be posted on the OVAL website the week before the event.

OVAL Board Voting Process

Multiple discussions were held for all the topics brought up by the OVAL Board over the voting process being established. The variety of subjects covered include voting period length, organizational voting practices, vote casting mediums, minimum quorum requirements, and the potential for Board "observer" roles.

Discussion

The first discussion covered the topic of voting duration. Initially, it had been proposed that all votes be resolved in a one week period. It was argued that the voting period should be established on a case-by-case basis due to the potential for different levels of effort being required from the Board member before coming to a voting decision. The OVAL Team agrees that this is a reasonable request and will revise the voting process document.

The next topic was the question of whether a vote would be given to each individual or organization on the Board. It was previously discussed with the Board that it made the most sense for organizations with

two Board members to act as one entity and only be allowed to cast one vote. There were no objections from the Board. Following this discussion, there was a question around the preferred method of voting, whether it should be done through email or an online poll. There was also a question on how to deal with multiple votes from a single voting entity. There was a general consensus that an email poll was sufficient to conduct voting. On the specific question of how to count votes, there were two options suggested. One Board member suggested that the last vote cast should count as the final vote. Another Board member cited this practice as a mistake since it encourages premature votes with the safety net that they can change it later. For this reason, it was suggested that the first vote should be counted with a documented process to approve invalidating the first vote if required. Handling these special situations on a case-by-case basis will encourage thoughtful voting. The MITRE Team will begin to document such a process. Regardless of the voting methods used, all Board members agreed that in the future these votes should be documented for the public to view, as it encourages transparency.

On the subject of determining a quorum, it was originally proposed that a simple majority of Board members would be required and a question was raised as to whether or not there are certain issues that would require more than a simple majority to reach a quorum. In the interest of keeping things simple, it was agreed upon that a simple majority of Board members would be required to reach a quorum, with the simple majority of those voting determining how to proceed on an issue. In the uncommon event of a tie, it makes sense to re-open the discussion. From the experience of several Board members who serve on the CVE Board, ties were usually attributed to lack of adequate discussion prior to voting.

The last major discussion was on the possibility of opening up the quarterly OVAL Board calls to outside observers. This option would provide the opportunity for those interested in the process of OVAL decisions to get a first-hand point of view of the relevant discussions. It would also allow Board members to bring in subject matter experts, from their organizations, to listen in on the discussion. These persons would remain non-Board members and would primarily be in a non-speaking role. Several Board members agreed that such an opportunity contributes to the open transparency of the OVAL Board and could be beneficial. It was noted that special precautions should be set in place to ensure that outside participants, with comments, did not take precedence over the main agenda for the Board meeting. It was also suggested that there should be a process to designate an “invited speaker” to discuss approved topics and be included in the agenda for a Board meeting.

Action Items

- MITRE to update the Board voting process document regarding voting duration, quorum, publishing results, and how to handle multiple votes per organization.
- MITRE to propose a process for allowing invited speakers and non-speaking observers to attend Board meetings.