OVAL Board Meeting (7/2/2012)

Attendees

Scott Armstrong - Symantec Corp.
Carl Banzhof - Rockport Systems
Chandrashekhar Basavanna - SecPod Technologies
Anthony Busciglio - Cisco Systems Inc.
Aharon Chernin - DTCC
Blake Frantz - Center for Internet Security
Morey Haber - eEye Digital Security
Robert Hollis - Threat Guard Inc.
Kent Landfield - McAfee Inc.
Steven Piliero - Center for Internet Security
Omar Santos - Cisco Systems Inc.
Amaresh Shirsat - Symantec Corp.
Michael Tan – Microsoft Corp.
Eric Walker - IBM Corp.

Jon Baker - MITRE
Matt Hansbury - MITRE
Dan Haynes - MITRE

Meeting Summary

Welcome

After introductions, the group was welcomed to the 2012 3nd quarter OVAL Board Meeting. One new board member was introduced to the group:

Amaresh Shirsat – Symantec Corporation

Status Update

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

OVAL Adoption

The notable activity for this quarter has been Positive Technologies completion of the OVAL Adoption Program Process for their OVAL Content Repository and eIQnetworks submitting an OVAL Adoption Declaration for their SecureVue product.

OVAL Language

The major focus regarding the OVAL Language has been thinking about the OVAL 5.11 release. The OVAL Board was also asked if they had any additional comments or thoughts about the IETF SACM effort and transitioning the OVAL Language to an international standards body. The OVAL Board was also

reminded that MITRE is really looking to them for guidance on whether or not such a transition makes sense.

Lastly, a recap of new capabilities currently being developed in the OVAL Language Sandbox was given. They include the macos-def:plist511_test, macos-def:pkgutil_test, win-def:license_test, NETCONF schema, JunOS schema, and Android schema. Some of these capabilities are also being developed in an OVAL Interpreter branch or other tools.

OVAL Interpreter

Version 5.10.1.2 of the OVAL Interpreter was released on May 7, 2012. This release features full support for the windows_view behavior for the registry-based tests and other bug fixes submitted by the community.

We also worked with Michael Tan and the rest of the Microsoft Team to get recommendations on implementing the windows_view behavior for the file-based tests. We need to go back and finish that work. Until then, we have a partial implementation available in the OVAL Interpreter branch "windows_view".

Lastly, the OVAL Board was reminded that we did not forget about the follow-up teleconference regarding the role, development, and licensing of the OVAL Interpreter, but, that MITRE needs more time to prepare for it so that we can have a productive discussion.

OVAL Repository

The OVAL Repository's definition count at the time of the call was 13,599 definitions. This quarter's top contributors were G2, Inc., SecPod Technologies, and Symantec Corporation. Since the last OVAL Board Call, a bug was reported over the oval-discussion-list[1] where the tool that generates the OVAL Repository downloads was producing invalid content. This bug has been fixed, however, if you notice any other issues with the content in the OVAL Repository downloads, please let us know.

Summary of OVAL Developer Days Sessions

The Developer Days sessions for OVAL represent a significant milestone in that the majority of the sessions will be led by vendors whereas previous sessions were primarily led by MITRE. A quick summary of the following Developer Days sessions was given.

- Lessons Learned Creating PowerShell Configuration Baselines
- OVAL for Mobile Devices
- OVAL for Network Devices
- OVAL for Database Vulnerability Assessment
- OVAL for Artifact Hunting
- Automated Checking of Windows User Configuration Settings

---

[1] http://making-security-measurable.1364806.n2.nabble.com/Repository-content-download-issue-tp7578402.html

Please see the Developer Days agenda[2] for additional information about these sessions.

Lastly, we would like to encourage everyone to review the read-ahead material[3] provided for each of the sessions to ensure productive discussions.

OVAL 5.11 Release Planning

At the last OVAL Board Call, you raised that you would like to see the following areas explored in the OVAL Language Sandbox.

- Scripting
- Network management & devices
- Improved database capabilities
- Mobile devices

In a follow-up message, we proposed that the following topics might also be good candidates for the OVAL 5.11 release:

- Entity casting
- Artifact hunting
- Core updates (bitwise function, path datatype, variable/function clean up, etc.)
- File test updates (better support parsing complex files and handling symlinks)

We have also been working to further explore some capabilities proposed over the oval-developer-list by the community including:

- Bitwise function
- macos-def:plist511_test
- macos-def:pkgutil_test
- win-def:license_test

With that said, we would really like to get your thoughts on what problems you are hearing from your customers and what are the requirements for the OVAL 5.11 release.

[Eric Walker]: It would be great if we could document how to handle the 32-bit/64-bit view issue on 64-bit Windows for content that was created before OVAL 5.10 which includes the window_view behavior.

[Jon Baker]: Yes, we can do that[4].

[Kent Landfield]: Are there plans to discuss OVAL 5.11 release goals at Developer Days?

---

[2] https://register.mitre.org/devdays/agenda.pdf

[3] http://oval.mitre.org/community/developer_days.html

[4] A tracker (#34690) has been created to address this issue.

[Jon Baker]: No, we are using Developer Days to work with the community to review and consider several vendor-led extensions of OVAL that are being developed in the OVAL Sandbox. Then after Developer Days, we plan to engage the OVAL Board and broader community in a discussion of the OVAL 5.11 release goals and timeline.

Action Items

- Follow-up conference call, with the OVAL Board, to discuss the role, development, and licensing of the OVAL Interpreter after Developer Days.
- Follow-up conference call, with the OVAL Community, to further discuss OVAL 5.11 release goals and timeline after Developer Days.