OVAL Board Meeting (10/19/2009)

Attendees

Chris Wood – Assuria Limited
Blake Frantz – Center for Internet Security (CIS)
Steven Piliero – Center for Internet Security (CIS)
Dennis Moreau – EMC
Scott Armstrong – Gideon Technologies, Inc.
Jonathan Frazier – Gideon Technologies, Inc.
Pai Peng – Hewlett Packard
Nils Puhlmann – Individual
Jay Graver – nCircle Network Security, Inc.
Timothy 'TK' Keanini – nCircle Network Security, Inc.
Dave Waltermire – NIST
Anton Chuvakin – Qualys, Inc.
Rob Hollis – ThreatGuard, Inc.

Jonathan Baker – MITRE
Andrew Buttner – MITRE
Danny Haynes – MITRE
Mike Lah – MITRE
Bryan Worrell – MITRE

Meeting Summary

Welcome

The group was welcomed and thanked for attending the 2009 3rd quarter OVAL Board Meeting. Board members were reminded of the effort to keep contact information up to date. Please confirm your information on the website and send any corrections to oval@mitre.org.

Status Update

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

- OVAL Language
  - OVAL Version 5.6 was released September 11, 2009. Thank you all for your hard work and support in successfully releasing a new version of the language
  - We feel like significant progress has been made, including new tests and an improved deprecation policy
- OVAL Interpreter
  - Support for Windows tests is almost complete. There will be continued development in order to provide support for the Linux and UNIX tests.
  - Work on Solaris and Mac OS X will begin later this Fall/Winter.

    - If any board members have advice or would like to help with the porting effort, please let us know. Any help would be greatly appreciated.
- OVAL Repository
    - We continue to receive a lot of content submissions. Thank you all for your efforts.
    - The "Top Contributors" this quarter were Gideon Technologies, Inc., Hewlett-Packard, and SecPod Technologies.
    - We are working on improving infrastructure in order to make submission turnaround faster.

OVAL Version 5.6 Release Process

For the 5.6 release, we required board approval before the release became official. For the 5.6 release, this approval process worked fairly well. There are approximately 35 members on the board, and there were approximately 12 approval responses. The board was then asked if the approval process could be refined by no longer focusing on the approval of a release, but instead allowing board members to veto or reject a release candidate. This suggested approach would allow any board member the ability to reject a release candidate. The consensus on the call was that the process is working well as is and a change is not needed for the next release of OVAL.

OVAL Version 5.7 (timeline)

Historically, releases occur 3 to 4 times per year and we have fallen behind that mark. Frequent releases and a planned release roadmap allow for steady incremental advances to the language while allowing organizations to target development activities for a specific future version of the language. We will once again work to define a release roadmap that accommodates the SCAP lifecycle and also ensures that the language continues to evolve.

There are two release proposals:

- Release 5.7 in February, and 5.8 in June. This allows some time before the end of the SCAP year. This would be just two releases over the course of the calendar year and ensure that there is plenty of time for implementation between the June release and the SCAP Lifecycle deadline in September.
- Release 5.7 in April, which also allows plenty of time before SCAP. However, there is a risk that the language will not evolve fast enough to meet community demand for support for new platforms.

After a brief discussion, it was agreed that quarterly releases seem to be too frequent; both difficult for vendors to keep up with, and resource intensive for the OVAL team. It is also agreed that it would be beneficial to track SCAP Validation and match the schedule as much as possible. Planning on two releases before the September SCAP lifecycle deadline is reasonable. The OVAL team will propose a release time line to include two releases over the next year and ensure ample time to fit with the SCAP timeline.

OVAL Validation Update

The OVAL team at MITRE continues to work on transitioning from OVAL Compatibility to NIST run OVAL Validation. A first draft of the test content that will be using in this program has been completed, and a set of OVAL test requirements are under development. As soon as the test requirements are reasonably complete they will be shared with the community for review.

Next Areas of Focus

With Version 5.6 official, the OVAL team at MITRE will be shifting focus to a number of items that were deferred as the team worked through the release.

Developer Days Actions

The following actions items were taken at the Security Automation Developer Days and were deferred until after the version 5.6 release. The OVAL team at MITRE will now work through these issues and solicit feedback from the board and the oval-developer-list as appropriate. More details on these action items can be found in the complete minutes from the Security Automation Developer Days .

- Deprecation Policy Clarification
  There is a need to clarify the deprecation policy and to state that Schematron rules do not fall under the deprecation policy

- Supporting Multiple Versions in Parallel
  There is a strong desire to support the development of multiple versions of the OVAL Language in parallel. This will require further discussion with the sponsor base in order to help support the needs of the OVAL Community. It might be more practical to support all components on the current release, and support selected components (schema and documentation) of past releases. We would also like to move on to a major release, but realize we must continue to support 5.x as it is used by SCAP and other organizations. We encourage members of the OVAL Community to post proposals for this topic on the oval-developer-list

- Defining a Major Version
  There is a need to clarify the difference between major and minor releases of the OVAL Language as well as define how much can we add to an OVAL release before it becomes a major change. We will take another pass at this document and seek feedback from the board

- OVAL Specification
  There are requests for an OVAL Language specification. Currently, we rely on the OVAL schemas and documents that contain high-level overviews, but, we have never had a formal specification. There have been requests for more formal and refined documentation which is indicative of the success of the OVAL Language

- OVAL Language Versioning Process & Implementation Review

There is a request to encode both the major and minor release versions within the XML namespaces that allows for the differentiation of tests across versions

Documentation Review

We plan to update the documents describing the different components (repository, tutorials, language, definitions, etc.) of OVAL. We want to improve this content and make it easier for people to learn and understand OVAL. If you see anything missing or having any suggestions for improving the documentation on the OVAL web site, please let us know by sending email to oval@mitre.org.

OVAL for System Querying/Reporting

At this year's Security Automation Developer Days, the idea of OVAL for system querying was discussed. The idea is to use existing OVAL constructs for simply retrieving system information for reporting purposes. For example, one could report on how many or which RPMs are installed on a system or what files exist in a directory. The idea is to generate a report on the system information without making any assertions about the state of the system. The OVAL team has started looking into this new application of the OVAL Language and will be proposing a schema and processing model for the purpose of reporting. This should be coming out over the oval-developer-list later this year.

Questions & Comments

A question was raised about a recent post to the oval-discussion-list regarding support for 64-bit versions of Windows in the OVAL Repository. The specific issue was described in the mailing list post and summarized on the call. There were several comments from the call participants suggesting that the issue may be solved by restructuring the Windows content to better support 32 bit applications running on 64 bit versions of Windows and also 64 bit applications running on 64 bit versions of Windows. This issue should be discussed and a content authoring proposal should be made on the oval-discussion-list so that all OVAL Repository users are aware of the issue and have an opportunity to weigh in on how best to restructure the content.