OVAL Board Meeting (07/12/2010)

Attendees

Nick Connor – Assuria Limited
Eric Walker – BigFix, Inc.
Jeff Spitulnik – BigFix, Inc.
Blake Frantz – Center for Internet Security (CIS)
Steven Piliero – Center for Internet Security (CIS)
Luis Nunez – CISCO
Melissa Albanese – DoD
Morey Haber – EEYE
Timothy 'TK' Keanini – nCircle Network Security, Inc.
Jay Graver – nCircle Network Security, Inc.
Kent Landfield – McAfee, Inc.
Michael Tan – Microsoft
Steve Grubb – Red Hat
Chandrashekhar B – SecPod Technologies
Rob Hollis – ThreatGuard, Inc.

Jonathan Baker – MITRE
Matt Hansbury – MITRE
Danny Haynes – MITRE
Mike Lah – MITRE
Nathan Przybyszewski – MITRE
Bryan Worrell – MITRE

Meeting Summary

Welcome

The group was welcomed to the 2010 3rd quarter OVAL Board Meeting. A new member, Jeff Spitulnik from Bigfix, was welcomed to the OVAL Board.

Status Report

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

OVAL Adoption

There are now 14 organizations and 21 products participating in the OVAL Adoption program. Novell is the latest addition to the OVAL Adoption Program. Novell is a primary source vendor who will host their own repository of OVAL Definitions, for security advisories, for all Novell products.

OVAL Language

The OVAL team has been busy working on Version 5.8 and has been publishing weekly drafts. A more detailed discussion of the OVAL Language and Version 5.8 will follow.

OVAL Interpreter

Version 5.7.1 of the OVAL Interpreter was released a few months ago with added support for n-tuples. Since this release, work has been done on the OVAL Interpreter in a few different areas. One of the changes was to merge the Solaris and Mac OS branches of the OVAL Interpreter into the trunk. Additionally, use of OpenSSL has been discontinued due to licensing issues and has been replaced by the native Windows API and the libgcrypt library on non-windows platforms. The libgcrypt library is also being looked at to replace the Windows API to reduce the amount of platform-specific code. Lastly, work on several Version 5.8 tests has begun ahead of the Version 5.8 release.

OVAL Repository

The OVAL Repository is growing quickly. It currently contains almost 7400 OVAL Definitions and another 2300+ will be added soon. The top contributors to the OVAL Repository this quarter are DTCC, SecPod Technologies, and Symantec, Inc.

Developer Days Recap

This year's Developer Days saw the best turnout so far. There were 86 registrants and about 75 registrants attended each day. Slides and minutes from the OVAL discussion have been distributed on the web site and the OVAL team has already begun moving forward with drafts and proposals based on this discussion. The slides and minutes, from the OVAL discussion, can be found at the following links.

OVAL Discussion Slides

http://oval.mitre.org/oval/about/OVAL-Dev-Days-06-14-2010.pdf

OVAL Discussion Minutes

http://oval.mitre.org/oval/about/OVAL_Developer_Days_2010_Minutes.pdf

The minutes from the entire Developer Days event will be available within a few days on the Making Security Measurable website (http://measurablesecurity.mitre.org/about/index.html). We continue to receive feedback that face-to-face developer discussions are helpful for continuing the development of OVAL. There are currently three OVAL events scheduled this year: the Security Automation Developer Days Winter 2010,Security Automation Developer Days 2010, and the 6th Annual IT Security Automation Conference to be held September 27-29, 2010. It is not yet certain if there will be a fourth event in the fall.

Version 5.8 Progress

A release candidate for Version 5.8 is currently scheduled for July 21. There is a good chance that this date will slip due to the number of change requests that we have recently received. The release date for Version 5.8 is set for August 18th, and this would also slip if the release candidate date slips.

Rob Hollis asked about the cutoff date for SCAP 1.2.

Jon Baker believes that the cutoff date is August 18, but, NIST is OK with a date slip. NIST is the source of several feature requests. Attention needs to be paid to this timeline to ensure that it makes sense.

Completing the core schema changes is the top priority and current focus of the Version 5.8 language development. The next priority is the addition of new tests, new entities to existing tests, and documentation. The goal is to get the core schemas stable as soon as possible since those changes will likely have the largest impact. Your review and feedback on the core changes, that have already been implemented, would be greatly appreciated.

Developer List

Due to the high volume of emails sent to the oval-developer-list, there is a concern that it may be too difficult to keep up with everything that is happening as we work on Version 5.8. Community input is greatly valued and we want to keep the community informed about any changes that are being made. Is there anything that can be done to help make the communication more manageable?

Rob Hollis feels that he has plenty of opportunity to follow and participate in discussions that are relevant to his interests, but it would be difficult to follow every topic.

Melissa Albanese thinks that the volume of email on the oval-developer-list is high, but the oval-board-list is much better controlled and appropriately used.

Jon Baker for this release we have done a better job capturing changes from draft to draft on the web site. We also expanded the tracker data on the web site in an effort to provide more insight into what is being changed from one draft to the next.

Versioning Methodology

A change to the versioning methodology has been proposed. Should backwards compatibility breaking changes be allowed for minor OVAL releases if they solve a critical issue? Any such changes would be approved on a case by case basis by the OVAL Board. Additionally, the oval-developer-list would also be consulted to make sure that the change is worth breaking compatibility.

Blake Frantz agreed with the new proposal.

Jon Baker asked if he had reviewed the examples.

Blake Frantz started to review them, but needs to look at them more. He asked if we can find out how many definitions will be affected by backwards compatibility breaking changes.

Jon Baker will try to find out those statistics. Jon also would like to send out the versioning methodology update to the oval-developer-list to garner wider feedback. By next week, Jon would like to update the versioning methodology on the web site and then begin to determine which items should be updated.

OVAL Reporting Schema

A draft for the OVAL Reporting Schema was submitted in February, but it was unable to get into the release of Version 5.7. As a result, it is currently aimed for the Version 5.8 release. There still have not been many comments from the community, but the review during Developer Days seemed to be positive. The OVAL Team is now looking for the OVAL Board's approval to add the new OVAL Reporting Schema to Version 5.8.

Questions

Steve Grubb has been reviewing the Version 5.8 drafts and raised a number of questions that he will raise on the oval-developer-list for community discussion.

Action Items

- OVAL Board feedback for Version 5.8 wanted.
- Small delay possible for Version 5.8.
- Feedback for Versioning Methodology changes wanted as soon as possible.
- Approval to add the OVAL reporting schema to Version 5.8 is needed.

Conclusion

Minutes for this meeting will be released later this week. Thank you for attending, and good bye.