OVAL Board Meeting (10/17/2011)

Attendees

Chandrashekhar B – SecPod Technologies
Alberto Bastos – Modulo
Aharon Chernin – DTCC
Blake Frantz – Center for Internet Security
Jonathan Frazier – Symantec Corporation
Rob Hollis – ThreatGuard, Inc.
Kent Landfield – McAfee, Inc.
Steven Piliero – Center for Internet Security
Michael Tan – Microsoft Corporation
Eric Walker – IBM
Dave Waltermire – NIST

Jonathan Baker – MITRE
Matt Hansbury – MITRE
Danny Haynes – MITRE
Jasen Jacobsen – MITRE
David Rothenberg – MITRE

Meeting Summary

Welcome

The group was welcomed to the 2011 4th quarter OVAL Board Meeting.

Status Report

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

OVAL Language & Interpreter

The OVAL team has recently released Version 5.10 of the OVAL Language. It has been out for just over a month and has received good feedback so far. The OVAL Interpreter was also updated for Version 5.10. Notable changes include the addition of the win-def:cmdlet_test, unix-def:sysctl_test, support for the unique and count functions as well as support for the applicability_check property. With this release, the Visual Studio project associated with the OVAL Interpreter, on Windows has been upgraded to Visual Studio 2010. The OVAL Test Content has also been updated to address a number of defects that were reported. We are in the process of moving the OVAL Test Content to be hosted on SourceForge so that the trackers and updates will be more accessible to the community.

Additionally, there will be a talk by Jon Baker on the changes made for OVAL Version 5.10 at the upcoming 7th Annual IT Security Automation Conference (ITSAC) on November 1st.

OVAL Adoption

The OVAL Adoption Program not experienced much change due to our focus on the 5.10 release. The notable activity has been the submission of an updated OVAL Adoption Declaration from Tripwire stating their plans to fully support OVAL and the completion of the OVAL Adoption Program Process by jOVAL.

With Version 5.10 complete, we will once again shift back towards expanding OVAL Adopters.

OVAL Repository

The OVAL Repository's definition count at the time of the call was 11,457 definitions. The repository tools have been updated to be in sync with Version 5.10. There have been a lot of submissions lately, with several big updates coming soon. This quarter's top contributors were G2, Inc., SecPod Technologies, and Symantec Corporation.

Main Topics

There has been an expressed desire for the OVAL community to take a step back before starting a Version 5.11 release in order to resolve several more strategic topics. This quarterly board call was used as the kick off for a series of OVAL Board discussions focused on the following topics. Each of these topics were briefly discussed to ensure that the board members had a shared understanding of them, identify any other strategic topics for discussion, and ensure that the OVAL Board could effectively move forward with more detailed discussions.

OVAL Language Specification

The team provided a reminder that the OVAL Language specification was published in conjunction with the Version 5.10 release and thanked Dave Waltermire for his inputs while encouraging others to read and review the document. Over the coming months, updates to improve the quality of the document will be published. The specification itself remains open to editorial change. This practice will not continue once the document becomes a bit more refined. We still plan to move away from documentation within the schema and replace that with the specification as the authoritative definition of the OVAL Language. However, we want to make sure that the OVAL community has some time to become familiar with the specification before we make this transition.

Discussion

During this topic, the Board brought up the following concerns.

Kent Landfield questioned whether it would be desirable to have the specification transitioned to become a NIST IR. Kent argued that transitioning to a NSIT IR would make OVAL more consistent with the other specifications that are used by SCAP.

Jon Baker addressed Kent's question about the possibility of a transition to a NIST IR. While DHS and NIST are discussing whether it would be appropriate to make such a change, it was Jon's idea that the language should stand as community based specification rather than a government specification.

Kent also pointed out that he has heard of concerns about the copyright that is maintained on the OVAL Language.

Jon Baker reminded the OVAL Board that the purpose of the copyright was to protect the OVAL Language and those that wish to make use of it. This is well documented in the OVAL terms of use

(https://oval.mitre.org/about/termsofuse.html). The OVAL Board was then asked to follow-up offline with the any questions or concerns about the copyright.

Next, Dave Waltermire asked how much of Version 5.10 is currently implemented by the OVAL Interpreter. The question was followed by another about whether there was documentation outlining the currently supported tests.

Danny Haynes reported that most of the core features added to Version 5.10 are incorporated within the Interpreter. It is primarily in updating support for the new tests where there is still some lag. The status of the currently supported OVAL Tests is documented on the SourceForge wiki page, accessible via http://sourceforge.net/apps/mediawiki/ovaldi/index.php?title=Supported_tests.

Requirements Collection and Decision Making

Currently, MITRE drives releases according to input from the community. These updates have incrementally added capabilities to the component schemas while largely leaving the core OVAL Language alone. For the past several years, the OVAL Language has been incrementally expanded to support new platforms and tests and only minor bug fixes or feature additions have been made to the core of the OVAL Language. We are currently working to improve the change request process and have documented this change request process, and the information that should be included with various change requests, as a start (http://oval.mitre.org/language/about/change_requests).

There have been requests for the OVAL Board to take a more active role in defining the purpose or goals for a release and which features are included in each release. A recommendation was made that the OVAL Board take feedback from the community and define goals and requirements for each release.

Discussion

Jon Baker discussed the current methodology of selecting priorities for minor releases, which has entailed a review of deferred items from previous releases and new minor feature requests from the community.

Kent Landfield feels that the current requirements gathering process is overly focused on developers that have tools or products that support the OVAL Language and would like to see the needs of end users become more influential in shaping release contents. As a result of not adequately gathering end user requirements, vendors have resorted to developing their own content and tools that provides capabilities outside the OVAL Language where solutions that leveraged OVAL might have been possible.

Jon Baker pointed out that the core schema has remained relatively unchanged since the Version 5.0 release and while most changes in the subsequent releases have come from platform schemas, the development team is willing to take on larger changes to the OVAL Language.

Jon asked for ideas on how to engage the end users in order to gather their requests and better understand the capabilities that they need.

Kent suggested obtaining a list of end users using SCAP enabled tools. From there, MITRE could have interviews or discussions with these contacts to gain an understanding of what the marketplace needs.

Establishing a Voting Mechanism

The idea of developing a formal voting mechanism to use when making decisions has been suggested in the past and deferred in favor of the rough consensus approach that is in active use. In order to further consider a formal voting mechanism the following questions must be answered: What would be voted on? Who votes? What does a vote mean?

Discussion

Some of the call participants agreed that the OVAL Board should take a more formal role in directing future OVAL changes. It was noted, by MITRE, that there is only loose documentation of the existing responsibilities of OVAL Board members. A proposal for a charter for the next version of the OVAL Language was made.

Dave Waltermire is in the process of trying to set up rooms to take advantage for the opportunity of a face-to-face meeting at ITSAC. This meeting could provide the chance for the OVAL Board to develop an initial charter for further review.

Release Cycle Timelines

The OVAL Board had previously agreed upon quarterly releases of the OVAL Language, while in practice there have been about two minor releases per year. This release cycle is closely related to the requirements gathering process for determining which requests are being included in a release. The OVAL Board was asked if there should be more frequent minor releases or if the current release cycle was acceptable.

Discussion

Some OVAL Board members felt that the timeline should stay in sync with the SCAP releases, in order to keep releases more focused and reduce vendor overhead caused by frequent language updates. Some vendors feel that it is difficult to define a product roadmap that allows them to stay in synch with OVAL releases. More frequent releases are seen by some as a distraction.

More interest was shown for a sandboxing environment for new language constructs, which could decrease the need for more frequent releases. Sandboxing capabilities could also be delivered without a full release.

Another solution would stem from the ensuring that all OVAL content was made available according to the least version that is required to support it. This would allow vendors to continue to make use of most OVAL content while they update their tools to support the current version of the language. By way of example, Red Hat continues to publish OVAL content using OVAL 5.3 without the need to update to Version 5.10. This ensures that their content is widely available to any tools that support any version of OVAL after 5.3.

Sandboxing

It is understood that there has been a great interest in providing a central location for experimental OVAL Language capabilities, for possible future inclusion into the release process. Further requirements for such a feature need to be gathered to ensure the need is properly addressed. Several high level thoughts have already been laid out over the years. The OVAL Board is encouraged to participate in discussing how these sandboxing capabilities will be set up, and help outline a process to transfer experimental features to a full

OVAL release. Follow-up sandboxing discussions were recommended to take place, in parallel, with other development talks in order to prevent another outcome from affecting this topic.

Scripting

The addition of scripting capabilities to OVAL has been discussed for the past several years. Progress has been made with the introduction of limited PowerShell support with the win-def:cmdlet_test. Additional scripting capabilities should be researched and tested within the planned sandbox environment. A planned first step would be to develop a script_test or similar any_test proposal, which was discussed at the May 11, 2011 call (http://making-security-measurable.1364806.n2.nabble.com/Community-Conference-Call-May-11-2011-at-11-00-AM-tt6317996.html).

Due to the delay on this solution, it has been brought to attention that several vendors have gone ahead and implemented their own unofficial scripting functionality. With the release of Version 5.10, there is now an opportunity to look into a scripting solution.

A more complete MITRE proposal based on feedback from the last call will help resume the scripting discussion in the future. Regarding the existing custom vendor scripting functionality, ideally the OVAL community can start discussions of scripting, in the OVAL Language, based upon the experiences and solutions that these vendors are currently using. OVAL Board members are encouraged to contribute their solutions to help advance this discussion.

Additional Device Support

OVAL Board and community guidance is relied upon heavily when considering which new platforms to support. Development of new component schemas should be driven by priorities set forth based on feedback from the OVAL Board members and community. The question of which platforms and devices should be added to the OVAL Language needs to be addressed.

Discussion

Having just discussed the desire of some board members to reduce the number of OVAL Language releases and gather requirements from end users, it is important to find an approach to adding in support for additional platforms at the request of end users and publish revisions to the OVAL Language in a manner that will allow vendors to implement support for the new additions.

In developing the OVAL Language specification, it was decided that these platform extensions would not be considered part of the official specification as a way to position the OVAL Language to become more easily extensible to new platforms.

The OVAL Board was also reminded that without input from the OVAL Board or end users, the OVAL team does not actively seek out new platforms. Most of the current tests and component schemas have been developed by the community.

Kent Landfield encouraged the group to focus first on how to integrate the current platform schemas with existing management capabilities. This would allow us to factor in the legacy perspective, and become more focused on a low level reference implementation that demonstrated the integration.

At the upcoming Open Group Conference (https://www.opengroup.us/dcconference/meetings.php?action=show&mtid=14) MITRE hopes to begin

discussions about possible integration or collaboration between the OVAL community and relevant Open Group efforts.

Language Expansion vs. Major Revision

A brief talk on the benefits of continuing the 5.x releases versus developing a new major 6.0 revision was covered. The effort of moving to a 6.0 release would require parallel support of the 5.x revisions, which is an acceptable compromise. Details of the major topics that would be included in a 6.0 release is planned to take place with a series of phone calls with the OVAL Board.

Incentivize Content Development

A long standing goal of OVAL is to "promote open and publicly available security content." Some primary source vendors distribute their own OVAL content. How can we support and encourage other vendors to develop content for their products? We have not provided enough of an incentive for major software vendors to bear the cost of developing and publishing this content. How can we motivate these vendors to publish such content?

Discussion

We have not engaged major vendors as well as we should have. The OVAL Board can help develop an approach or strategy to ensure that there is sufficient incentive to create and publish standard content. Minimally, the OVAL Board members could influence this by advocating within their own organizations that their products have OVAL content freely available for inventory, patch checking, and configuration checking uses cases.

Kent Landfield pointed out that as a vendor there is little incentive to share custom content with direct competitors. He says that the content won't always be free since the vendors would love to recoup their content development costs, and that this content has a marketable value.

The goal from the beginning was to promote sharing of open standardized content. Without a clear indication of how, it is still vital to get past the negative incentive to share.

OVAL Content Development Topics

MITRE would like to work with the OVAL Board to determine how best to reduce the content development cost. The community continues to show interest in the development of a content editor, despite the fact that several open source editors are available. How are the existing editors falling short and could an editor be developed that would greatly simplify content development?

The OVAL Board should also consider how we can improve the overall quality of content. There have been numerous talks about content development best practices, but there is still little public guidance on creating good OVAL content. As part of the OVAL Repository effort, we should work together to provide more comprehensive tools and documentation on creating good OVAL content. MITRE needs the help of the OVAL Board and the community to do this well.

OVAL Outreach Topics

Within the US Government, the OVAL Language is fairly widely used. How do we leverage this exposure to gain broader industry and international adoption? MITRE would like the help of the OVAL Board to develop an outreach strategy for the effort.

Other Comments or Questions

The board was asked if there were any other topics that did not make the list for the call.

Discussion

Dave Waltermire suggested that OVAL will need to address the issues of multiple instantiation and the functionality problems that multiple instantiation causes for other security automation specifications that make use of OVAL.

Conclusion

The call was concluded with an outline of the goal to meet in person at ITSAC. In preparation for this meeting, we will work with the OVAL Board to identify the correct topic for discussion. If possible, a phone conference line will be provided for those that cannot attend in person.