OVAL Board Meeting (4/13/2009)

Attendees

Jonathan Baker – MITRE
Andrew Buttner – MITRE
Daniel Haynes - MITRE
Bryan Worrell – MITRE
Melissa Albanese – DoD
Scott Armstrong – Gideon Technologies, Inc.
Jonathan Frazier – Gideon Technologies, Inc.
Kent Landfield – McAfee
Anton Chuvakin – Qualys, Inc.
Jay Graver - nCircle Network Security, Inc.
Morey Haber – eEye Digital Security
Chan Yoon - NetIQ Corporation
Jon Lane – Lumension Security
Nils Puhlmann – Individual
Anton Chuvakin – Qualys, Inc.
Alex Quilter – Hewlett Packard
Pai Peng – Hewlett Packard
Dennis Moreau – ConfigureSoft
David Waltermire - Booz Allen Hamilton
Steven Piliero – CIS
Randy Taylor – ThreatGuard, Inc.
Chandrashekhar B – SecPod Technologies
Morey Haber - eEye Digital Security

Agenda

- Welcome
- Status Update
    - OVAL Language
    - OVAL Interpreter
    - OVAL Repository
- OVAL Developer Days Planning
- OVAL Compatibility/Adoption Update
- Versioning Process Update
- Release Roadmap
- Questions/Concerns

Meeting Summary

Welcome

After introductions the group was welcomed to the 2009 2nd quarter OVAL Board Meeting. One new board member was introduced to the group:

- Chandrashekhar B – SecPod Technologies

Status Update

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

- OVAL Language
  - We have completed the needed updates and clarifications to the release process and are ready to resume work on version 5.6.
  - A lot of work has been done on the documentation on the language web site to address the concerns on the versioning and deprecation policy (e.g., supporting old versions of the language to minimize impact on vendors).
- OVAL Interpreter
  - Work is being done to improve Windows support with a new build coming in the next few weeks. Moving forward, we plan to continue to improve Linux support and develop a port to Solaris all in an effort to enable the SCAP Validation Program to test on Windows , Linux, and Solaris systems.

- OVAL Repository
  - The OVAL Repository continues to be current for all Windows advisories. There are active Sun, HPUX, and Apple (content for the latest Safari issues and other Apple software products) and related content contributions as well. Over the past four months, we have had vulnerability definitions submitted for two Windows zero day vulnerabilities (IE and PowerPoint). It is great to have the repository up and current before the patches move out.

OVAL Developer Days Planning

OVAL Developer Days has been in the late spring/early summer time frame for several years now. At the last couple of events, we have received requests to extend the event to all of the SCAP standards and protocols. With this is mind, we are planning this year's OVAL Developer Days as part of a week-long SCAP Developer Days event at MITRE's Bedford campus. At this point, we are unsure how much time OVAL will get and/or use on the agenda. We are currently thinking OVAL will have at least a half day. There will be a lot of time spent on the review of SCAP and the criteria for inclusion of a new effort in SCAP. This is going to be a technical event for developers and standards developers.

We have considered both a linear and track format for the sessions. We want to look at all of the efforts in order to determine what to include. Please use the OVAL-Developer-List as a forum for suggesting and discussing topics for OVAL at this year's event. The agenda is not fixed at this point. XCCDF, OVAL, and other efforts will likely be covered.

OVAL Compatibility/Adoption Update

We continue to work closely with NIST to complete the transition to a NIST-run OVAL Validation Program. Through SCAP's existing OVAL testing, NIST and MITRE have received feedback about the need for expanding the breadth and depth of the OVAL testing. This has led us to reevaluate the testing program and again delay the launch of a standalone OVAL program. We hope to only stand up a standalone OVAL Validation program when we are confident that it will meet the end user needs. This is causing us to invest time and effort into:

- expanded test suites and example content
- OVAL Interpreter development to support validation testing
- enhanced test requirements to ensure proper coverage of OVAL Language constructs

We are expecting this delay to push the start date of the standalone OVAL Validation Program at NIST back a few months until summer 2009. We need to understand what end users need and expect from an OVAL Validated product. We plan to look to the Board and vendors supporting OVAL for guidance here.

- What impact will this 3-6-month delay have?
  It is not certain what the level of work is required for writing test content, updating the interpreter, and refining the test requirements. We are currently working on scoping this effort.

- Will there be coverage for platforms other than Windows?
  A first priority will be ensuring that testing for Windows platforms is complete. At this point, we are thinking that we will require products to support all tests defined in the OVAL Language for each platform a product claims support. Support for other platforms will follow. We will likely focus on Red Hat, Solaris, and then OSX.

- How does the expanded testing relate to SCAP Validation Program?
  SCAP has a validation program life cycle in place. The SCAP Validation Program will be open to revision sometime in the next few months and we'll try to identify improvements for the process.

Versioning Process

In response to the discussion related to the versioning process, we have better documented and clarified our current process. Since our last meeting, we have completed and published a new deprecation policy. We have reviewed, clarified, and reorganized the existing documentation related to how we version the language and the review process utilized for new versions of the language. Please take a look at these documents and let us know if you have any additional questions or comments. Our goal is to make sure that the community has complete visibility into how the process works and to ensure that the process meets the community needs. The following is a link to these documents:

http://oval.mitre.org/language/about/index.html

We've used feedback to generate three standalone documents on the OVAL website (URL directly above). The most significant change has been the addition of a formal deprecation policy. This addition will likely be the most impactful change on the OVAL Language schemas in the next minor version since we will populate all of this new deprecation information for each item that is currently deprecated. Again, please review the new documents and give us any additional feedback you may have.

Release Roadmap

At the January meeting, we decided to hold off on a next release (minor or major) until after the versioning process was clarified. We are now ready to move forward with a next release. We have attempted to align the timeline with the SCAP Validation Program's Lifecycle to ensure that SCAP has the opportunity to leverage the latest release of OVAL when their validation program is updated in September. The timeline that we suggest for version 5.6 is:

- DRAFT May 14
- RELEASE CANDIDATE July 17
- OFFICIAL August 14

We need to be cognizant of the SCAP Validation Program lifecycle and work to ensure that we have a release in good shape for the 1 September 2009 deadline. The suggested timeline will allow for this and give us plenty of time to produce a high quality release that could be included in SCAP in September.

Version 6 Discussion

We would also like to discuss version 6. We have previously been compelled to hold off on version 6 due to concerns about too much version churn for organizations supporting and using OVAL as well as concerns related to the interaction of the current version of OVAL and the version of OVAL used in SCAP. Now that the OVAL Language versioning process has been clarified, and NIST has developed a formalized SCAP Validation lifecycle, we should be able to proceed without causing version churn pain for NIST and participating vendors. We would like to understand the board's perspective on this.

The major points of the discussion focused around the relationship between SCAP required OVAL and the official version of OVAL, conversion of the OVAL Repository to version 6.0, and support for 5.x content, the need for a better understanding of what will be in version 6.0, and the acknowledgement that the drivers for version 6.0 should include the end users that buy and use OVAL Validated products. Below are some of the major questions and remarks from this discussion:

- Kent Landfield – What version of OVAL will SCAP use?
- Drew Buttner - What is your feeling about going forward with version 6.0, even if SCAP does not adopt it immediately? We might have trouble supporting both versions simultaneously.
- Anton Chuvakin - It is understandable and probably good that SCAP will be somewhat behind the current OVAL version.

- Jon Baker - Can the repository go right to version 6.0 and convert all the existing content to when version 6.0 is released? In the past we have converted the OVAL Repository on the day that the new version of the language became official. We have always tried to make sure that the interpreter and the repository were current when we released a new version of the language.
- Kent Landfield - We will need to cover what the SCAP DTR covers for OVAL plus the newer stuff. Is the content of the 5.x repository going to be taken and put into version 6.0, where there will be no hope of finding an archive for that?

- Randy Taylor – Since SCAP will be relying on version 5.x for some period of time any content transition must support two versions for awhile (5.6 and 6.0).

- Drew Buttner - How important it is to have a repository for version 6.0 out there right away, even if it isn't going to heavily used?
- Kent Landfield - Is there no way to provide a repository that supports multiple versions of OVAL? This will allow the content to migrate to remain in version 5.x without conversion? We are making repositories too version-specific.

- Jon Lane – With regard to data transfer to version 6.0, are you thinking of writing a conversion utility so that the data can be converted forward?
- Jon Baker – In the past we have written a onetime conversion utility to migrate content from one version to the next.

- Melissa Albanese – Will tool vendors be expected to support both version 5.x and version 6.0?
- Kent Landfield - Keep the focus on the content based on the SCAP DTR; if they dictate we go to version 6.0, then we do it.

- Dave Waltermire - What about the end users? We need to understand what the end users need from OVAL Validated products.
- Jon Baker - We have great representation from vendors and developers on the board and need their voice, but we also need to understand what the end users are asking for.
- Melissa Albanese - I could live with a tool that supported only version 6.0.
- Dave Waltermire - Well what if you have content that is not written in version 6.0?
- Melissa Albanese – Ideally tools would support both 5.x and 6.0.

- Kent Landfield - Should we be scheduling a date for version 6.0? Does a requirements document exist for us to use so that we have vetted requirements in hand while we work?
- Drew Buttner - The best we have is tracker information which allows end users to understand the difference between 5.x and 6.0.
- Kent Landfield - A draft generated in the near future would be expedited by an MRD (marketing requirements document). That might be drawn up to define the purpose of the release. Once we've got that done, it answers a lot of the questions.

- Melissa Albanese - On version 6.0; what is the timeline for the next one going into the SCAP?
- Jon Baker - September 2010 is the next time the SCAP DTR will be open for modification; it would be great for SCAP to be able to pick up version 6.x at that time. SCAP is getting ready to produce a validation program lifecycle. Given that the next opportunity for changing the version of OVAL in SCAP will be September 2010 we have plenty of time to get version 6.0 right.

The consensus from the group was that without a better understanding of what version 6.0 will look like it is very difficult to answer many of our questions. There was general agreement that we need to start working on version 6.0 to better understand the impact it will have on the OVAL Repository, SCAP, and end users. With this in mind, we will be developing a lengthy release timeline in the near future and will begin posting drafts of version 6.0 for all to consider. Once we get the version 5.6 release under way, we will begin work on the version 6.0 release with a goal, of having a 6.0 or 6.1 release ready for the 2010 revision of the SCAP Validation Program's DTR.

Questions/Concerns

- In late April ,OVAL will be part of the "Making Security Measurable" booth at the RSA conference in San Francisco, staffed by MITRE folks in the same location as last year.
- Melissa Albanese - Thanks so much for taking another look at validation; it is a great help and well worth the wait.