An Introduction to OVAL™ Compatibility

Version 5.0

The MITRE Corporation

June 2006

Introduction

OVAL Compatibility is a program established to develop consistency within the security community regarding the use and implementation of OVAL. The main goal of the compatibility program is to create a set of guidelines that will help enforce a standard implementation. An offshoot of this is that users are able to distinguish between, and have confidence in, compatible products knowing that the implementation of OVAL coincides with the standard set forth.

This document introduces OVAL Compatibility and outlines exactly what the OVAL Compatibility Program is trying to accomplish. The process one would follow to become OVAL-Compatible is also explained.

OVAL Overview

Open Vulnerability and Assessment Language (OVAL™) is an international, information security, community effort to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language.

The OVAL community has developed three schemas written in Extensible Markup Language (XML) to serve as the framework and vocabulary of the OVAL Language. These schemas correspond to the three steps of the assessment process: an OVAL System Characteristics schema for representing system information, an OVAL Definition schema for expressing a specific machine state, and an OVAL Results schema for reporting the results of an assessment.

Content written in the OVAL Language is located in one of the many repositories found within the community. One such repository, known as the OVAL Repository, is hosted by The MITRE Corporation. It is the central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL definitions. Each definition in the OVAL Repository determines whether a specified software vulnerability, configuration issue, program, or patch is present on a system.

The information security community contributes to the development of OVAL by participating in the creation of the OVAL Language on the OVAL Developers Forum and by writing definitions for the OVAL Repository through the OVAL Community Forum. An OVAL Board consisting of representatives from a broad spectrum of industry, academia, and government organizations from around the world oversees and approves the OVAL Language and monitors the posting of the definitions hosted on the OVAL Web site. This means that the OVAL, which is funded by US-CERT at the U.S. Department of Homeland Security for the benefit of the community, reflects the insights and combined expertise of the broadest possible collection of security and system administration professionals worldwide.

What Is OVAL Compatibility

OVAL Compatibility means that a tool, service, Web site, database, or advisory/alert incorporates OVAL in a pre-defined and standard way. A product or service is considered OVAL-Compatible if it uses OVAL as appropriate for communicating details of vulnerabilities, patches, security configuration settings, and other machine states.

When considering a capability for OVAL Compatibility it must be determined to which schema(s) the capability complies (OVAL System Characteristics, OVAL Definition, and/or OVAL Results), and whether the capability is a "Producer" that generates data that conforms to a specific schema, a "Consumer" that utilizes an existing data set for some purpose, or both.

Some examples of producers are a software inventory tool that gathers OVAL Systems Characteristics information, a software vendor who creates draft OVAL definitions in their security bulletins, or a vulnerability assessment tool that outputs its test findings in accordance to the OVAL Results Schema. Examples of consumers are a vulnerability assessment tool that draws in the OVAL System Characteristics file and then runs OVAL Definitions against the information, rather than directly gathering the information at run-time; a remediation tool that imports the OVAL Results; or an organizational status reporting tool that uses the OVAL Results to provide information on conformance with policy.

Examples of OVAL Compatibility

The following are some examples of entities that would meet the initial requirements of OVAL Compatibility:

A tool that relies upon OVAL Definitions to conduct a vulnerability assessment of a system is called an OVAL-Compatible scanning tool. OVAL Definitions follow one of the component-centric OVAL schemas; these schemas describe the structure and vocabulary of the OVAL definitions for each supported platform (i.e., Microsoft Windows, Red Hat Linux, Sun Solaris, Debian Linux, etc.). In addition to using OVAL Definitions for defining its tests, an OVAL-Compatible scanning tool is able to store its test results following the OVAL Results schema structure.

Another area of OVAL Compatibility covers the collection of the information that is used to evaluate the OVAL definition tests. An OVAL-Compatible scanning tool can collect or read the various file system information and settings as it scans systems, or the information can be collected ahead of time and stored in a file that follows the OVAL Systems Characteristics schema. Then the OVAL-Compatible scanner can read in the data from the OVAL Systems Characteristics file and evaluate the OVAL Definitions against the stored data. Tools that collect and export OVAL Systems Characteristics files are part of another category of OVAL Compatibility.

Similarly, applications that can ingest OVAL Results files are part of third type of OVAL-Compatible tools. For example, a tool that uses OVAL Results files to construct an enterprise report on vulnerability status, or recommends remediation approaches, would be in this third type of OVAL Compatibility. Likewise, a certification and accreditation report creation tool that uses OVAL Results files would also be in this category.

The fourth type of OVAL Compatibility is for organizations that create and publish OVAL Definitions in advisories and bulletins, including the software suppliers, security research organizations, or security vendors that create OVAL Definitions of how to test for the presence of the vulnerability they are describing in their advisory/bulletin.

Benefits of OVAL Compatibility

Adopting OVAL-Compatible products and services benefits organizations working to secure their enterprises, and providing compatible products benefits the vendors that help them do it. Some of the benefits of using OVAL-Compatible products and services are:

- Compatibility provides a method for consistent and reproducible information assurance metrics from your systems.
- Compatibility lets you know definitively that your network security products and services are interoperable and hence work together to protect your enterprise.
- Use of OVAL Definitions in compatible products and services provides you with confidence that the issues being tested are actually present on the system (with fewer false positives).
- Compatibility ensures that tools have undergone some amount of testing to meet the requirements.
- The compatibility process is well documented and open, thus providing users with details about the tool's OVAL implementation.
- Compatibility provides vendors with something that distinguishes them from competition – thus encouraging compatibility through the industry.
- Compatibility provides users with a standard against which to measure tools when making purchasing decisions.

Some of the benefits for vendors integrating OVAL into their products and services are:

- Customers want products and services that can work together, and compatibility enables interoperability.
- Compatibility signifies your organization incorporates community standards that benefit your customers.
- Gain a competitive edge over companies that aren't participating.
- OVAL's standardized baseline data allows you to focus your R&D on the advanced and higher-level aspects of your product, increasing ROI.
- Standardized OVAL data can be used as a second level of assessment to your proprietary methods and offered as a product enhancement.
- Incorporating standardized OVAL Definitions that test for software vulnerabilities, compliance issues, programs, and patches could serve as enhancements to your existing products or services, or as the foundation of new ones.
- Leverage existing OVAL content that has been produced by OVAL-Compatible software vendors and the OVAL Repository.
- Use of the OVAL-Compatible logo on your Web site, product packaging, etc., serves as a purchase incentive for prospective customers, informing them that your product/service is certified as "officially" compatible with a growing industry standard.

The OVAL Compatibility Program

For a product or service to gain official OVAL Compatibility, it must complete the OVAL Compatibility Program. The program involves three phases, each of which must be completed before proceeding to the next phase. The first phase, called the Declaration Phase, consists of registering an organization's declaration of intent to make its product(s) and/or service(s) OVAL-Compatible. The second phase, called the Implementation Phase, requires the completion of a questionnaire that specifically looks at the details of how the organization has satisfied the "Requirements and Recommendations for OVAL Compatibility." The third phase, called the Evaluation Phase, involves correctness testing where the product or service is put through a rigorous set of tests to prove conformance to the standard.

Organizations that successfully complete all three phases will be included in a branding program that offers an official OVAL-Compatible Product/Service logo to indicate compatibility. The logo is authorized for use on Web sites, product packaging, publicity and marketing materials, trade show and other signage, etc.

Program Summary

Phase 1 – Declaration of OVAL Compatibility

1. Review the "Requirements and Recommendations for OVAL Compatibility" document posted on the OVAL Web site.
2. Email oval@mitre.org and request the "OVAL Compatibility Declaration Form."
3. Review Authority emails you the declaration form.
4. Complete the form and return it to oval@mitre.org.
5. The form is reviewed by the Review Authority.
6. The product or service is added to the list of Declarations to be OVAL-Compatible on the OVAL Web site.

Phase 2 – Implementation of OVAL Compatibility

1. Complete the integration of OVAL into the product or service.
2. Email oval@mitre.org and request the "OVAL Compatibility Questionnaire."
3. Review Authority emails you the compatibility questionnaire .
4. Complete the questionnaire and return it to oval@mitre.org.
5. The completed questionnaire is reviewed by the Review Authority.
6. The questionnaire is posted on the OVAL Web site.

Phase 3 – Evaluation of OVAL Compatibility

1. Send an email to oval@mitre.org requesting the "Procedures for OVAL Compatibility Correctness Testing" document and review it.
2. Send an email to oval@mitre.org requesting correctness testing for your product or service.
3. Review Authority responds with a date and location for correctness testing.
4. You assist the Review Authority with the correctness testing when necessary (this may involve travel).
5. After testing is complete, the product or service is listed as “Officially OVAL-Compatible” on the Compatible Products and Services page and
6. The organization receives a compatibility certificate and is included in the branding program.

Phase 1 – Declaration of OVAL Compatibility

The first phase of the OVAL Compatibility Program consists of an organization reviewing the "Requirements and Recommendations for OVAL Compatibility" which is available on the OVAL Web site, and then making a declaration stating that their product or service fulfills, or will fulfill, those requirements.

Phase 1 of the compatibility program is initiated by requesting the "OVAL Compatibility Declaration Form" from oval@mitre.org. This form is filled out and then sent back to oval@mitre.org. Once the declaration is reviewed, the following information will be listed on the OVAL Web site (Note: Declarations will only be posted for products or services that are commercially available.):

- Organization name
- Web site address
- Quote: a brief paragraph of how and why the organization is participating in the OVAL effort
- Product/Service name with URL link to organization's product page
- Product/Service Type: category of information security product or service
- Capability: the specific OVAL capability of the product or service
- Status: the compatibility is listed as Available or Planned

At this time you will also receive a "Compatible Product/Service Organization Welcome Kit" with items for your Web site including:

- OVAL link button that can be used on their Web site to link to the OVAL main site.
- OVAL Compatibility FAQ questions and answers.
- OVAL Compatibility glossary terms and definitions.
- A brief HTML document describing OVAL.

Phase 2 – Implementation of OVAL Compatibility

The second phase of the compatibility program involves the integration of OVAL into an organization's product(s) and the completion of the "OVAL Compatibility Questionnaire". Please note that only those organizations that completed the declaration phase can move on to the implementation phase.

Once a declaration of OVAL Compatibility is made, an organization should work with their development team to integrate the language into their products and services. After the integration is complete, the "OVAL Compatibility Questionnaire" can be requested by sending an email to oval@mitre.org. This questionnaire requires that the organization state specific and verifiable details about how it has satisfied the compatibility requirements. Upon completion, the form is submitted to MITRE by sending it back to oval@mitre.org.

At this time, MITRE will review the responses to the questionnaire and notify the organization of any potential areas of concern. Once both MITRE and the organization are satisfied with the questionnaire, MITRE will update the compatible products/services page on the OVAL Web site. Please note that this includes posting the questionnaire

and its answers. The publication of the organization's questionnaire on the OVAL Web site allows end users and prospective customers to compare how different products satisfy the requirements and decide which are best.

Phase 3 – Evaluation of OVAL Compatibility

The third phase of the compatibility program involves an evaluation process. To begin this phase, organizations must have completed their declaration(s), and must have submitted a satisfactory questionnaire. Once this has been accomplished, an organization can start phase 3 by reviewing the "Procedures for OVAL Compatibility Correctness Testing" document which is available on the OVAL Web site that outlines the plan and expectations surrounding correctness testing.

Correctness testing allows MITRE to verify that the organization's implementation of OVAL meets the compatibility requirements, as stated in the "Requirements and Recommendations for OVAL Compatibility" document. It usually involves a face-to-face meeting where MITRE exercises the organization's product and verifies the claims made in the questionnaire. To request correctness testing, send an email to oval@mitre.org. The organization will then be contacted by MITRE and the details necessary for scheduling a testing session will be worked out.

Once correctness testing has been completed, MITRE will complete its review of evaluation and then notify the organization of the results of the correctness test. If no issues were raised during this test and MITRE has deemed it a success, then the product or service will officially gain OVAL-Compatible status.

At this time, the organization will receive an official OVAL-Compatible logo to indicate compatibility. Logo use recommendations and restrictions will be supplied at that time. In addition, the organization's product will be listed on the Compatible Products and Service page on the OVAL Web site.

Additional Information

For any additional information please read the "Requirements and Recommendations for OVAL Compatibility" located on the OVAL Web site at http://oval.mitre.org or send an email to oval@mitre.org.