Requirements and Recommendations for OVAL™ Compatibility

Version 5.0

Introduction

OVAL Compatibility is a program established to develop consistency within the security community regarding the use and implementation of OVAL. The compatibility program's main goal is to create a set of guidelines that will help enforce a standard implementation. A by-product 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 outlines the requirements and recommendations that need to be satisfied in order for a tool, service, Web site, database, or advisory/alert to be deemed OVAL-Compatible.

OVAL Overview

Open Vulnerability and Assessment Language (OVAL™) is an international, information security, community standard 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.

Definitions

The following terms are used throughout this document.

Capability - a security tool, database, Web site, advisory, or service that needs to exchange data relating to vulnerabilities, patches, security configuration settings, and other machine states

User - a consumer (or potential consumer) of a capability

Owner - the creator, seller, or maintainer of a capability

Producers - a capability that generates data that conforms to one of the OVAL schemas (i.e., an OVAL Definition producer conforms to the OVAL Definition schema, an OVAL System Characteristics producer conforms to the OVAL System Characteristics schema, and an OVAL Results producer conforms to the OVAL Results schema.)

Consumers - a capability that utilizes existing OVAL conformant data for some purpose

Repository - an implicit or explicit collection of security elements that supports a capability, e.g., a vulnerability database, the set of signatures in an assessment tool, or Web site

Correctness Testing - the process of determining whether a capability is OVAL-Compatible

Test Results - data representing the outcome of correctness testing.

Review Authority - an entity that performs Correctness Testing and is authorized to grant OVAL-Compatible status (MITRE is the only Review Authority at this time)

Common Compatibility Requirements

The following requirements apply to all tools, services, Web sites, databases, advisories/alerts, checklists, etc. regardless of the category for which they are seeking compatibility. If the *capability* does not satisfy all applicable requirements, then the *owner* shall not be granted OVAL Compatibility. In addition, the owner shall not advertise OVAL Compatibility until the review authority has granted such.

General

These requirements deal with general aspects of the OVAL Compatibility.

1.1 -- The *owner* shall be a valid legal entity, i.e., an organization or a specific individual, with a valid phone number, email address, and street address.

1.2 -- The *owner* shall agree to abide by all of the mandatory OVAL Compatibility Requirements, which includes the mandatory requirements for the specific type of capability.

1.3 -- The *capability* shall provide additional value or information beyond that which is provided in OVAL itself. Therefore, forwarding or providing references to a single source of OVAL Definitions that have been created by someone else is not considered to be OVAL-Compatible.

1.4 -- The *capability* shall be available to the public, or to a set of consumers.

1.5 -- The *owner* shall provide the *review authority* with a technical point of contact who is qualified to answer questions regarding any OVAL-related functionality of the capability and coordinate the preparation of the *capability* for the *correctness testing*.

1.6 -- The *owner* shall provide the *review authority* with a completed "OVAL Compatibility Questionnaire Form". This form will be sent once the declaration process has been satisfied. Please see the section "How to Declare Your Product or Service OVAL-Compatible" for more information.

1.7 -- The *owner* shall provide the *review authority* with free access to items needed to perform correctness testing, including the *test results* and/or the *repository*, in order to determine compliance with all associated requirements.

1.8 -- The *owner* shall work with the *review authority* to make the *capability* available for *correctness testing*.

1.9 -- As a part of being awarded OVAL-Compatible status, the *owner* shall agree to support the *review authority* in follow-on testing activities, where appropriate types of files will be exchanged with other organizations attempting to prove the correctness of their *capability*. This will be managed by the *review authority* and kept to reasonable levels of effort for all involved.

1.10 -- The *capability* shall clearly state the schema(s) and version with which it is compatible.

Correctness

OVAL facilitates information exchange only if the data encoded in OVAL is presented and used correctly. Therefore, OVAL-Compatible *capabilities* must meet minimum correctness requirements.

2.1 -- Any use or translation of OVAL data shall reflect the same logic as the original OVAL Document.

2.2 -- The *owner* shall have in place a means for the *user* to submit correctness errors found in the use of OVAL and in any OVAL content being produced by the *capability*.

2.3 -- The *owner* shall have a plan in place to address any correctness errors reported to it.

2.4 -- The *owner* shall address any correctness errors reported to it within a reasonable time frame after the error was initially reported.

Documentation

The following requirements apply to documentation that is provided with an OVAL-Compatible capability.

3.1 -- The *capability* shall include in its documentation a brief description of OVAL and OVAL Compatibility, which can include verbatim portions of documents from the OVAL Web site.

3.2 -- The *capability* shall clearly state in its documentation any component schemas or individual tests that it does not support. For example, if a tool applying for OVAL Compatibility as a definition consumer does not know how to deal with metabase tests, then the tool's documentation shall state this incompatibility.

3.3 -- The *capability* shall clearly state in its documentation the procedure a *user* must follow to submit correctness errors found in any OVAL content being produced by the *capability*.

3.4 -- If the documentation included with the *capability* includes an index, then it shall include references to OVAL-related documentation under the term "OVAL."

Validity

OVAL-Compatible tools are required to work with valid documents. This helps to ensure that information is being formatted correctly and that the structure of the document follows the OVAL Language standard.

4.1 -- The *capability* shall validate all OVAL content (both produced and consumed) using the W3C schema validation against the version of the OVAL Language with which it is stated to comply.

4.2 -- The *capability* shall report any W3C schema validation errors to the user.

4.3 -- The *capability* should validate all OVAL content (both produced and consumed) using the Schematron validation against the version of the OVAL Language with which it is stated to comply.

4.4 -- The *capability* should report any W3C schema validation errors to the user.

Specific Compatibility Requirements

The following requirements apply to specific parts of the OVAL Language and only apply to *capabilities* that are looking to gain OVAL Compatibility in that specific category.

OVAL Definition Schema

These requirements apply to all capabilities that intend to make use of the OVAL Definition Schema.

Consumer Requirements

These requirements apply to all capabilities that intend to consume information in the OVAL Definition Schema format.

5.1.1 -- The *user* shall be able to determine which OVAL Definitions are being consumed. The goal is to make sure the *user* can identify the different definitions that are being used by the capability.

5.1.2 -- The *user* shall be able to examine the details of each OVAL Definition being consumed. This can be as simple as allowing the *user* to open an XML file that contains all the OVAL Definitions. The point of this requirement is to make sure that the OVAL Definitions are open to the *user* allowing them to see how a specific issue is being tested.

5.1.3 -- If the *capability* does not consume OVAL Definitions at runtime, the *owner* shall document the process by which a *user* can submit OVAL Definitions to the *owner* for interpretation by the capability. This includes stating how quickly definitions submitted to the *owner* are made available to the *capability*.

5.1.4 -- The *capability* shall be capable of interpreting the logic within each OVAL Definition and subsequent OVAL Test in accordance with the stated logical operators.

Producer Requirements

These requirements apply to all capabilities that intend to generate information in the OVAL Definition Schema format.

5.2.1 -- All newly created definitions, tests, objects, states, and variables shall contain a unique ID with respect to all other definitions, tests, objects, states, and variables in the OVAL Community.

5.2.2 -- The definition meta-data shall be consistent with the definition content - e.g., the family shouldn't be 'windows' if the tests are examining Red Hat RPM's.

5.2.3 -- A capability that produces an OVAL Definition to cover a specific vulnerability shall include, when available, a CVE name as a reference.

OVAL System Characteristics Schema

These requirements apply to all capabilities that intend to make use of the OVAL System Characteristics Schema.

Consumer Requirements

These requirements apply to all capabilities that intend to consume information in the OVAL System Characteristics Schema format.

6.1.1 -- The *user* shall be able to determine which systems are being described by the consumed data.

6.1.2 -- The *user* shall be able to examine the details of the OVAL System Characteristics file being consumed. This can be as simple as allowing the *user* to open the XML file. The point of this requirement is to make sure that the OVAL System Characteristics used are open to the *user* allowing them to examine the data being examined.

6.1.3 -- If the *capability* does not consume OVAL System Characteristics files at runtime, the *owner* shall document the process by which a *user* can submit OVAL System Characteristics files to the *owner* for interpretation by the capability. This includes stating how quickly files submitted to the *owner* are made available to the *capability*.

Producer Requirements

These requirements apply to all capabilities that intend to generate information in the OVAL System Characteristics Schema format.

6.2.1 -- The *capability* shall use a unique item ID (unique on a per file basis) for each specific system characteristic item it collects.

6.2.2 -- The *capability* shall generate system characteristics items that contain the exact system configuration values gathered at the time the *capability* executed against the system.

OVAL Results Schema

These requirements apply to all capabilities that intend to make use of the OVAL Results Schema.

Consumer Requirements

These requirements apply to all capabilities that intend to consume information in the OVAL Results Schema format.

7.1.1 -- For each system defined in the OVAL Result file being consumed, the *user* shall be able to determine the specific OVAL Definitions that are being reported on.

7.1.2 -- The *user* shall be able to examine the details of the OVAL Results file being consumed. This can be as simple as allowing the *user* to open the XML file. The point of this requirement is to make sure that the OVAL Results used are open to the *user* allowing them to examine the data being reported.

7.1.3 -- If the *capability* does not consume OVAL Results files at runtime, the *owner* shall document the process by which a *user* can submit OVAL Results files to the *owner* for interpretation by the capability. This includes stating how quickly files submitted to the *owner* are made available to the *capability*.

Producer Requirements

These requirements apply to all capabilities that intend to generate information in the OVAL Results Schema format.

7.2.1 -- The *capability* shall generate accurate and predictable results when using a specific set of definition content and system characteristic content or system state information.

7.2.2 -- The results generated by the *capability* shall be repeatable when given the same set of definition content and system characteristics content or system state information as input.

7.2.3 -- When an OVAL Definition has been evaluated more than once on a single system, each time with different values for the variables, the OVAL Results file shall include unique variable instance values for each individual case.

7.2.4 -- A *capability* shall use a result of "not evaluated" for all definitions part of the original OVAL Definition file that are not being reported on.

Review Authority Requirements

The following are requirements pertaining to OVAL Compatibility that the *review authority* must adhere to.

8.1 -- The *review authority* shall clearly identify the version of the compatibility requirements document and the version of the OVAL Language that was used to determine compatibility for the *capability*.

8.2 -- The *review authority* shall define and publish sample test materials prior to *correctness testing*.

8.3 -- The *review authority* shall publicize the schedule for *correctness testing* as much in advance as possible.

8.4 -- The *review authority* shall provide a point-of-contact for arranging *correctness testing* for *capabilities* declaring support for OVAL that have completed the "OVAL Compatibility Questionnaire Form".

8.5 -- The *review authority* may re-test a compatible *capability* at the discretion of the *review authority*.

Revocation of Compatibility

If the *review authority* has verified that a *capability* is OVAL-Compatible, but at a later time the *review authority* has evidence that the requirements are no longer being met, then the *review authority* may revoke its approval and the *capability* will no longer be OVAL-Compatible. The following are requirements the *review authority* must follow in order to revoke compatibility.

9.1 -- The *review authority* shall provide the *capability owner* with a warning of revocation at least two (2) months before revocation is scheduled to occur.

9.2 -- The *review authority* may delay the date of revocation.

9.3 -- If the *review authority* has found that the actions or claims of the owner are intentionally misleading, then the review authority may skip the warning period. The *review authority* may interpret the phrase "intentionally misleading" as it wishes.

9.4 -- If the *review authority* finds that the actions of the *owner* with respect to the compatibility requirements are intentionally misleading, then revocation shall last a minimum of one year.

9.4 -- The *review authority* shall identify the specific requirement(s) that are not being met.

9.5 -- If the *owner* believes that the requirements are being met, then the *owner* shall respond to the warning of revocation by providing specific details that indicate why the *capability* meets the requirements under question.

9.6 -- If the *owner* modifies the *capability* so that it complies with the requirements in question during the warning period, then the *review authority* should end the revocation action for the *capability*.

9.7 -- The *review authority* shall publicize that OVAL Compatibility has been revoked for the *capability*.

9.8 -- The *review authority* may publicize the reason for revocation.

How to Declare Your Product or Service OVAL-Compatible

To begin the OVAL Compatibility process, send an email to oval@mitre.org requesting the "OVAL Compatibility Declaration Form". This form, along with a copy of the "Requirements and Recommendations for OVAL Compatibility" will be sent to you for review. Once the form has been filled out, email it back to oval@mitre.org.

Additional Information

For any additional information see the "An Introduction to OVAL Compatibility" document located on the OVAL Web site at http://oval.mitre.org or send an email to oval@mitre.org.