OVAL™ Compatibility Correctness Testing

Version 5.0

Introduction

The final phase of the OVAL Compatibility Program is Correctness Testing, which must be passed by a capability in order to achieve official OVAL-Compatible status. Please see the document "An Introduction to OVAL Compatibility" for more information about the OVAL Compatibility Program and the different phases involved.

The purpose of Correctness Testing is to ensure that companies, and their capabilities, use OVAL as defined by the OVAL Community. This aids other organizations in knowing which capabilities can be used to interface with one another. To be certified by the Review Authority as OVAL Compatible, a capability must run through the procedures defined in this document.

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.

Testing Infrastructure

The process defined later in this document relies on the following infrastructure: This infrastructure will be provided by the Review Authority for the testing session.

Testbed

The Review Authority shall provide a number of systems connected by a local network for the review. All necessary access to testbed machines shall be provided, as well as time to install any required software, test and troubleshoot. The testbed will have internet connectivity. An organization that requires a connection with the internet should communicate with the Review Authority before the testing session to make sure everything will be setup in a manner that meets the capabilities requirements.

The actual makeup of the testbed will vary, but a typical testbed would consist of 5-10 systems with various OS and applications installed. The testbed will be adjusted for each Correctness Testing session by the Review Authority to appropriately serve the involved capabilities.

Definition Test Suite

The Definition Test Suite is a collection of OVAL definitions that shall be provided by the Review Authority. It will be provided in the form of a single XML file that contains all the definitions. This file may be broken up into individual files if necessary. Should a candidate require advance knowledge of definitions (e.g. to convert to an internal format), they should contact the Review Authority one week prior to the testing session and the Definition Test Suite will be made available.

For examples of previous test suites, visit the OVAL web site at:

http://oval.mitre.org/compatible/about/correctness.html

System Characteristics Test Suite

The System Characteristics Test Suite shall be a collection of OVAL System Characteristic data provided by the Review Authority. It will be provided in the form of a single XML file that contains information about each system in the Testbed. This file can not be given out early.

For examples of previous test suites, visit the OVAL web site at:

http://oval.mitre.org/compatible/about/correctness.html

Results Test Suite

The Results Test Suite shall be a collection of OVAL Results provided by the Review Authority. It will be provided in the form of a single XML files that contains the results of an evaluation of the Testbed. This file can not be given out early.

For examples of previous test suites, visit the OVAL web site at:

http://oval.mitre.org/compatible/about/correctness.html

Testing Procedures

OVAL Compatibility consists of six different areas. During Phase I of the OVAL Compatibility Program, each capability declared compliance with one or more of these areas. Correctness Testing for each area is outlined below.

OVAL Definition Consumer Testing

Candidate OVAL Definition Consumers will first be asked by the Review Authority to demonstrate within the capability, validation of the Definition Test Suite against the schema version with which it is stated to comply. Once the test suite has been validated, the candidate's capability shall evaluate the definitions included in the Definition Test Suite using the provided Testbed for system information. Each candidate will be expected to produce results (not necessarily OVAL Results) for each definition in the Definition Test Suite. If a capability does not support a particular platform, then this should be presented in the results. Also, all errors during evaluation should be included in the results provided.

The results of a Candidate's assessment shall be compared with a pre-determined assessment of the target machine(s) by the Review Authority. At a minimum, the capabilities results must be identified by the corresponding OVAL Definition ID and contain the true/false/unknown/error answer determined by the evaluation. Results for individual OVAL tests included in these definitions are highly desirable and will aid in understanding any discrepancies.

Capabilities that do not consume OVAL Definitions at runtime shall educate the Review Authority about the process by which they consume OVAL Definition submissions and then transfer them to their capability.

The candidate capability passes the test and is considered a Compatible OVAL Definition Consumer if the results obtained by evaluating the Definition Test Suite exactly match the official results produced by the Review Authority's predetermined assessment.

OVAL Definition Producer Testing

Candidate OVAL Definition Producers shall make available to the Review Authority all available OVAL Definitions they have produced to date. The Review Authority will choose a sampling of definitions to consider and shall validate the selected definitions against the appropriate version of the OVAL Language to ensure stated compliance. The Review Authority will also confirm that all OVAL IDs are unique with respect to both the candidate and the OVAL Community as a whole.

In addition, the Review Authority will verify that an appropriate reference exists for each submitted definition (CVE for vulnerability class definitions) and that all metadata and tests contained within each OVAL definition are consistent with the Review Authority's guidelines for a complete definition.

OVAL Results Consumer Testing

Candidate OVAL Results Consumers will first be asked by the Review Authority to demonstrate within the capability, validation of the Results Test Suite against the schema version with which it is stated to comply. Once the test suite has been validated, the candidate's capability shall illustrate to the Review Authority how the OVAL Results are incorporated. For each OVAL Definition in the Results Test Suite, the candidate must show successful importation of the included OVAL-ID and the associated OVAL Result. This information must be linked to an appropriate system identifier and displayed to the user.

OVAL Results Producer Testing

Candidate OVAL Results Producers shall produce OVAL Results files corresponding to the evaluation of the testbed using the OVAL Definitions comprising the Definition Test Suite. The Review Authority may require multiple copies of OVAL Results be generated from the same target machine (or machine data set if using OVAL System Characteristics files) to review repeatability of the OVAL Results.

The Review Authority will validate the candidate's OVAL Results against the appropriate version of the OVAL Language. The OVAL Results will then be compared to an OVAL Results file generated by the Review Authority. The purpose of this comparison is to review the OVAL Results file for accuracy and correctness.

If a candidate's capability performs assessment against some stock models of machine states, (clean installs of OSs, etc) rather than actual systems in the Testbed, there are additional requirements. The candidate must provide valid System Characteristics files with the machine states used with the Definition Test Suite to produce the Results. This will allow the Review Authority to verify that the Results are correct. The Review Authority, at its sole discretion, may allow the candidate to generate the OVAL Results using their own models instead of the System Characteristics files provided by the Review Authority.

OVAL System Characteristics Consumer Testing

Candidate OVAL System Characteristic Consumers will first be asked by the Review Authority to demonstrate within the capability, validation of the System Characteristics Test Suite against the schema version with which it is stated to comply. Once the test suite has been validated, the candidate's capability shall run the Review Authority through the process by which they consume OVAL System Characteristics, and how the information is then used within their application. The purpose of this is to make a correctness assessment about the use of the OVAL System Characteristics file.

OVAL System Characteristics Producer Testing

Candidate OVAL System Characteristics Producers will be asked to produce OVAL System Characteristics files corresponding to the evaluation of the Testbed. The Review Authority may require more than one OVAL System Characteristics generation from a given Testbed system to review repeatability of the OVAL System Characteristics, or to assure a given set of changes to the system are displayed by the capability.

The Review Authority will validate the candidate's OVAL System Characteristics files against the appropriate version of the OVAL Language. They will then be compared to an OVAL System Characteristics file generated by the Review Authority. The purpose of this comparison is to review the OVAL System Characteristics file for accuracy and correctness.

Review Outcome

The Review Authority shall provide the Candidate with a detailed report on the outcome of the OVAL Compatibility Test. The Candidate shall be given the opportunity to explain any discrepancies to the Review Authority. The Review Authority, at its sole discretion, may choose to consider or reject these explanations before making an official ruling on the outcome of the capabilities OVAL compatibility. At that point, all rulings made by the Review Authority are final.

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.