NIST

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Interagency Report
7669(Draft)

Open Vulnerability and Assessment Language (OVAL®) Validation Program Test Requirements (DRAFT)

John Banghart
Stephen Quinn
David Waltermire

NIST Interagency Report 7669 (Draft)

Open Vulnerability and Assessment Language (OVAL) Validation Program Test Requirements (DRAFT)

John Banghart
Stephen Quinn
David Waltermire

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

March 2010

U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Dr. Patrick D. Gallagher, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards (Draft)
17 pages (Feb. 2010)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgements

The authors, John Banghart, Stephen Quinn, and Dave Waltermire of the National Institute of Standards and Technology (NIST), would like to thank the many people that reviewed and contributed to this document. In particular, the following individuals provided invaluable input and feedback: Jon Baker (MITRE) and Drew Buttner (MITRE).

Abstract

This report defines the requirements and associated test procedures necessary for products to achieve one or more Open Vulnerability and Assessment Language (OVAL) Validations. Validation is awarded based on testing a defined set of OVAL capabilities by independent laboratories that have been accredited for OVAL testing by the NIST National Voluntary Laboratory Accreditation Program (NVLAP).

Audience

The audiences for the OVAL Validation Program test requirements include laboratories that are accredited to conduct OVAL product testing for the program, vendors that are interested in receiving OVAL Validation for their products, and organizations seeking to deploy OVAL tools in their environments. The laboratories use the information in this report to guide their testing and to ensure that all necessary requirements are met by a product before recommending to NIST that the product be awarded the requested Validation. Vendors may use the information in this report to understand what features their products must have to be eligible to receive any of the OVAL Validations. Organizations use the information to gain insight into the criteria that products being considered for procurement must meet to be validated.

Comments

Comments on this report are welcome. Please direct them to IR7669comments@nist.gov.

Table of Contents

List of Tables

1. Introduction

Open Vulnerability and Assessment Language (OVAL) is an information security community standard to promote open and publicly available security content, and to standardize the transfer of this information across security tools and services. The OVAL Language is an XML specification for exchanging technical details on how to check systems for security-related software flaws, configuration issues, and patches. The OVAL 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 the assessment. In this way, OVAL enables open and publicly available security content and standardizes the transfer of this content across the entire spectrum of information security tools and services. OVAL is maintained by the MITRE Corporation. The capabilities and requirements described in this document have been derived from the OVAL Language Use Cases (http://oval.mitre.org/language/about/use_cases.html).

1.1 Purpose and Scope of the Program

The NIST OVAL Validation Program is designed to test the ability of products to use the features and functionality defined in the OVAL Language. An information technology (IT) product vendor can obtain one or more OVAL Validations for a product. These validations are based on the test requirements defined in this document, which cover four distinct but related validations based on product functionality. Note that OVAL Validation for a particular capability may not require all the tests that are defined. Table 1-2 provides a matrix indicating which tests are required for each capability.

Under the OVAL Validation Program, independent laboratories are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP) (http://ts.nist.gov/standards/accreditation/index.cfm) to conduct OVAL Validation testing. Accreditation requirements are defined in NIST Handbook 150 and NIST Handbook 150-17. Independent laboratories conduct the tests contained in this document on IT security products and deliver the results to NIST. Based on the independent laboratory test report, the OVAL Validation Program then validates the product under test. The validation certificates awarded to vendor products are publicly posted on the NIST OVAL Validated Products web page (http://nvd.nist.gov/scapproducts.cfm).[1]

OVAL Validation will focus on evaluating specific versions of vendor products based on the platforms they support. Validation certificates will be awarded on a platform-by-platform basis for the version of the product that was validated.

1.2 Supported Version of OVAL (OVAL 5.6)

These test requirements were developed for OVAL Version 5.6.

Specification: http://oval.mitre.org/language/

Schema Location: http://oval.mitre.org/language/download/schema/version5.6/index.html

1.3 Superseded Compatibility Programs

The OVAL Validation Program supersedes the OVAL Compatibility Program, run by the MITRE Corporation. NIST and MITRE have worked closely to streamline this transition. The OVAL Validation

[1] The OVAL Validation Program does not provide physical certificates to the participating vendors.

Program described in this document is independent but complementary to the MITRE OVAL Adoption Program.[2] These two programs work together to promote the proper use of OVAL.

2. Conventions and Definitions

2.1 Document Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in Request for Comment (RFC) 2119[3].

As necessary, the availability of an Internet connection, wireless or wired, during the evaluation of each test requirement will be indicated by the statements “permitted” or “not permitted”. When “permitted” is indicated, a product may make full use of any available network connection to access Internet-based resources. If “not permitted” is indicated, then no Internet network connectivity shall be provided during evaluation of the test procedure. Every effort has been made in the test requirements to avoid mandating that the capability to run in the presence or absence of Internet connectivity be supported by a product. Use of an Internet connection in some test procedures is disallowed to ensure that the functionality being evaluated in the tool exists directly within the tool and not as the result of utilizing an Internet-based capability. Access to a local area network (LAN) shall be allowed in all tests to support client-server based implementations.

2.2 Common Definitions

The following definitions represent key terms used in this document.

Comparison Utility: A utility provided to the accredited laboratory testers by NIST for use in the validation of product data sets as defined by certain testing requirements.

Deprecation: The OVAL Language defines a process by which constructs may be deprecated and eventually removed from the language. Deprecated constructs are considered valid components of the OVAL Language until they are officially removed.[4]

Derived Test Requirement/Test Requirement: A statement of requirement, needed information, and associated test procedures necessary to test a specific OVAL feature.

Import: A process available to end-users by which an OVAL xml file can be loaded manually into the vendor product. During this process, the vendor process may optionally translate this file into a proprietary format.

Machine-Readable: Tool output that is in a structured format, typically XML, which can be consumed by another program using consistent processing logic.

Major Revision: Modifications to the OVAL Language that invalidate OVAL content written for previous versions of the current major version will result in a major version change.[5]

[2] More information about the OVAL Adoption Program is available here: http://oval.mitre.org/adoption/

[3] For more information, please refer to Internet Engineering Task Force (IETF) RFC 2119, Key words for use in RFCs to Indicate Requirement Levels. S. Bradner. March 1997, http://www.ietf.org/rfc/rfc2119.txt?number=2119.

[4] For more information, please refer to the OVAL Language Deprecation policy: http://oval.mitre.org/language/about/deprecation.html

Minor Revision: Modifications the OVAL Language that do not invalidate OVAL content written for previous versions of the current major version will result in a minor version change. All changes made in a minor version will be backward compatible with the previous minor versions within a given major version.[4]

OVAL ID: An identifier for a specific OVAL Definition that conforms to the format for OVAL IDs. For more information please see the OVAL specification reference in Section 2.1.

Product: A security software application, appliance, or security database that has one or more capabilities.

Product Output: Information produced by a product. This includes the product user interface, human-readable reports, and machine-readable reports. There are no constraints on the format. When this output is evaluated in a test procedure, either all or specific forms of output will be sampled as indicated by the test procedure.

Reference Product: A product provided to accredited laboratory testers by NIST for use as a baseline for testing requirements. The product exhibits the behavior that is deemed to be correct.

Capability: A specific function or functions of a product. The supported OVAL Capabilities are defined in Table 1-1.

Target Platform: The target operating system or application on which a vendor product will be evaluated using a platform-specific validation lab test suite. These platform-specific test suites consist of specialized OVAL content used to perform the test procedures defined in this document.

[5] For more information, please refer to the OVAL Language versioning methodology: http://oval.mitre.org/language/about/versioning.html

2.3 OVAL Validation Capabilities

The OVAL Validation program is divided into five Capabilities, each targeting a different use case. This enables members of the OVAL Community to easily find the capability that best suits their need. Table 1-1 lists the capabilities.

Table 1-1. OVAL Validation Capabilities

Capability	Definition
System Characteristics Producer	A product that generates a valid OVAL System Characteristics file based on the details of a system
Definition Repository	A repository of OVAL Definitions made available to the community (free or pay)
Definition Evaluator	A product that uses an OVAL Definition to guide evaluation and produces OVAL Results (full results) as output
Results Consumer	A product that accepts OVAL Results as input and either displays those results to the user, or uses the results to perform some action

2.4 Supported Target Platforms

OVAL Validations are awarded on a per platform basis. Each platform is grouped with other like platforms and these platform groups are then associated with the set of OVAL Language schemas that must be supported for a given platform group. A product is expected to implement all applicable OVAL Language constructs defined in the schemas associated with the platform group that it supports. Additionally a product may be validated on any number of platforms.

The table below lists the supported target platforms and the corresponding platform groups for which OVAL Validations are available.

Table 1-2. OVAL Platform Groups

OVAL Platform Groups
Linux
Red Hat EL 5
Mac OS
Apple Mac OSX 10.6
Microsoft Windows
Windows XP
Window Vista
Windows 7
Windows Server 2003
Windows Server 2008
Sun Solaris
Solaris 10

The table below lists all of the OVAL platform groups and the applicable OVAL Language schemas.

Table 1-3. OVAL Schemas Mapped to Platform Groups

OVAL Schema	OVAL Platform Groups			
	Linux	Mac OS	Microsoft Windows	Sun Solaris
oval-common-schema-xsd	X	X	X	X
oval-definitions-schema.xsd	X	X	X	X
oval-resutls-schema.xsd	X	X	X	X
oval-system-characteristics-schema.xsd	X	X	X	X
independent-definitions-schema-xsd independent- system-characteristics -schema-xsd	X	X	X	X
linux-definitions-schema.xsd linux- system-characteristics -schema.xsd	X			
macos-definitions-schema.xsd macos- system-characteristics -schema.xsd		X		
solaris-definitions-schema.xsd solaris- system-characteristics -schema.xsd				X
unix-definitions-schema.xsd unix- system-characteristics -schema.xsd	X	X		X
windows-definitions-schema.xsd windows- system-characteristics -schema.xsd			X	

3. Vendor Product Validation Testing Requirements

The following guidelines must be followed by all vendors seeking validation of a product:

1. Vendors must provide the required vendor information detailed within the applicable derived test requirements.

2. Several OVAL tests require OVAL content as input. Therefore, vendor products may be required to import OVAL content.

Vendors may update validated products, but the new version is **not** automatically validated. To validate an updated product, the vendor must send documentation to the laboratory that performed the existing validation explaining the validation-related changes to the product. This statement will be posted publicly by NIST with the product's validation and thus must not contain proprietary information. The vendor may provide the laboratory additional proprietary details that will not be sent to NIST and will not be publicly posted.

The laboratory will review the changes, list the impacted testing requirements, and retest those requirements. The laboratory will then provide NIST a test report that summarizes how the product was changed and provides relevant test results. NIST will review the report and make a decision regarding whether to validate the updated product. If validation is granted, the newly validated product will have the same expiration date as the originally validated product since full testing of all requirements was not performed. Because of this, vendors may wish to fully retest an updated product if the expiration date is near and if a significant amount of retesting is required for the update.

4. Derived Test Requirements

The following requirements have been derived from the OVAL Adoption Technical Use Cases and the Requirements and Recommendations for OVAL Adoption. The table below indicates which requirements shall be tested for each defined OVAL Capability.

Table 1-4. OVAL Requirements per Validation Capability

OVAL Requirement	System Characteristics Producer	Definition Repository	Definition Evaluator	Results Consumer
R.1	X	X	X	X
R.2	X	X	X	X
R.3	X	X	X	X
R.4	X	X	X	X
R.5			X	
R.6	X		X	
R.7				X
R.8		X		
R.9		X		
R.10		X		

4.1 Derived Test Requirements

R.1: The product's documentation (printed or electronic) must state that it uses OVAL and explain relevant details to the users of the product.

Required Vendor Information

V.1: The vendor shall indicate where in the product documentation information regarding the use of OVAL can be found. This may be a physical document or a static electronic document (e.g., a PDF or help file).

Required Test Procedures

Internet Connectivity: Permitted

T.1: The tester shall visually inspect the product documentation to verify that information regarding the product's use of OVAL is present and to verify that the OVAL documentation is in a location accessible to any user of the product. This test does not involve judging the quality of the documentation or its accuracy.

R.2: The vendor must assert that the product implements the OVAL specification and provide a high-level summary of the implementation approach.

Required Vendor Information

V.2: The vendor shall provide a 150 to 500-word English language document to the accredited validation lab that asserts that the product implements support for one or more of the capabilities defined above, and provides a high-level summary of the implementation approach. This content will be used on NIST and MITRE web pages to explain details about each validated product and thus must contain only information that is to be publicly released. If applicable, this document shall include information about what product functionality uses OVAL versus what product functionality does not.

Required Test Procedures

Internet Connectivity: Permitted

T.2.1: The tester shall inspect the provided documentation to verify that the documentation asserts that the product implements the OVAL specification and provides a high-level summary of the implementation approach. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements OVAL.

T.2.2: The tester shall verify that the provided documentation is an English language document consisting of 150 to 500 words.

R.3: The product shall report and optionally reject OVAL content that is invalid according to the OVAL Language including constructs and restrictions specified in both XML Schema and Schematron schema.

Required Vendor Information

V.3: The vendor shall provide instructions on how validation of OVAL content is performed and where errors from validation are displayed within the product output.

Required Test Procedure

Internet Connectivity: Not permitted

T.3.1 (Definition Evaluator): The tester shall attempt to import known invalid OVAL Definition content into the vendor's product and examine the product output to validate that the product reports and optionally rejects the content as invalid according to the OVAL Definition schema and Schematron schema.

T.3.2 (Definition Repository): The tester shall attempt to import known invalid OVAL Definition content into the vendor's product and examine the product output to validate that the product reports and optionally rejects the content as invalid according to the OVAL Definition schema and Schematron schema.

T.3.3 (System Characteristics Producer): If the product produces OVAL System Characteristics based on input OVAL Definition documents, the tester shall attempt to import known invalid OVAL Definition content into the vendor product and examine the product output to validate that the product reports and optionally rejects the content as invalid according to the OVAL Definition schema and Schematron schema. If the product does not use OVAL Definition documents to produce OVAL System Characteristics no verification is needed by the tester.

T.3.4 (Results Consumer): The tester shall attempt to import known invalid OVAL Full Results content into the vendor product and examine the product output to validate that the product reports and optionally rejects the content as invalid according to the OVAL Results schema and Schematron schema.

R.4: The product output shall enable users to view the XML OVAL Definitions being consumed by the tool (e.g., within the product user interface or through an XML dump of the OVAL Definitions to a file).

Required Vendor Information

V.4: The vendor shall provide instructions on how the user can view the XML OVAL Definitions being consumed by the product.

Required Test Procedure

Internet Connectivity: Not permitted

T.4: The tester shall follow the provided vendor instructions to view the XML OVAL Definitions being consumed by the product and verify that access is provided as stated.

R.5: The product shall be able to correctly evaluate a valid OVAL Definition document against target systems of the target platform type and produce an result document using the full OVAL Results XML format with a definition result for each definition in the input OVAL Definition document.

Required Vendor Information

V.5: The vendor shall provide instructions on how a valid OVAL Definition file can be imported into the product for evaluation. The vendor shall also provide instructions on where the resultant full OVAL Results XML output can be viewed by the tester.

For T.5.5, the vendor shall indicate how two or more values can be specified for a variable used by one OVAL Definition.

Required Test Procedure

Internet Connectivity: Not permitted

T.5.1: The tester shall run the tool using valid OVAL Definitions documents against the target systems of the target platform type. The results shall be compared against results from the OVAL reference implementation and they must produce the same pass/fail result for each OVAL Definition and criteria contained within the definition.

T.5.2: The tester shall validate the resulting full OVAL Results XML output using the OVAL Results XML Schema and Schematron schema. Both of these validations must not produce any errors.

T.5.3: The tester shall validate that the resulting full OVAL Results XML is available for viewing by the user.

T.5.4: The tester shall inspect the product output and compare it against the reference results to ensure the proper use of result types ("not evaluated", "error", etc.).

T.5.5: When an OVAL Definition has been evaluated more than once on a single target system, each time with different values for the variables, the tester shall validate that the full OVAL Results XML file includes unique variable instance values for each individual case.

R.6: The product shall generate system characteristics items that contain the exact system configuration values gathered at the time the product assessed the target system.

Required Vendor Information

V.6: The vendor shall provide the lab with product documentation (printed or electronic) indicating where the full OVAL Result XML or OVAL System Characteristics XML output can be viewed within the product output.

Required Test Procedure

Internet Connectivity: Not permitted

T.6.1: (Definition Evaluator): The tester shall visually inspect the product output and compare the full OVAL Result XML to the expected results given the known configuration of the target platform.

T.6.2: (System Characteristics Producer): The tester shall visually inspect the product output and compare the OVAL System Characteristics XML output to the expected output given the known configuration of the target platform.

R.7: The vendor shall document the process by which a user can import OVAL Results documents for interpretation by the product.

Required Vendor Information

V.7: The vendor shall provide product documentation (printed or electronic) to the lab indicating how users can import OVAL Results files for interpretation by the product.

Required Test Procedure

Internet Connectivity: Not permitted

T.7: Using the vendor-provided documentation, the tester shall import one or more OVAL Results files for interpretation by the product. The tester shall confirm that this process works as documented by the vendor.

R.8: All definitions, tests, objects, states, and variables within the product shall contain a unique OVAL ID with respect to all other definitions, tests, objects, states, and variables in the OVAL Community.

Required Vendor Information

V.8: The vendor shall provide product documentation (printed or electronic) to the lab indicating where in the product output the unique ID for all definitions, tests, objects, states, and variables can be viewed.

Required Test Procedure

Internet Connectivity: Not permitted

T.8.1: The tester shall select a random sample of definitions, tests, objects, states, and variables (10%, up to 30, of each) from the product output and ensure that no duplicate IDs exists.

T.8.2: The tester shall validate that the OVAL ID is valid according to the OVAL ID naming specification as expressed in the OVAL schema.

R.9: Each definition shall keep the same OVAL ID across its existence.

Required Vendor Information

V.9: The vendor shall provide product documentation (printed or electronic) to the lab indicating where in the product output the definition OVAL ID can be viewed. This shall include reference to all components of the product in which the ID is displayed.

Required Test Procedure

Internet Connectivity: Not permitted

T.9: The tester shall select a random sample of IDs from all components of the product output (10%, up to 30) and verify that the ID remains consistent across all instances. For example, if the product produces output as both an XML file and within a user interface, both must be examined to ensure that the OVAL Definition ID is the same for the definition under review.

R.10: The definition metadata shall be consistent with the definition content (e.g., the family should not be “windows” if the tests are examining Linux.)

Required Vendor Information

V.10: The vendor shall provide product documentation (printed or electronic) to the lab indicating where in the product output the definitions and associated metadata can be viewed.

Required Test Procedure

Internet Connectivity: Not permitted

T.10: The tester shall select a random sample of IDs with metadata from the product output (10%, up to 30%) and verify that the metadata is consistent with the content of the definition.

5. Appendix A—Acronyms and Abbreviations

This appendix contains selected acronyms and abbreviations used in the publication.

DTR	Derived Test Requirements
ID	Identifier
IETF	Internet Engineering Task Force
IR	Interagency Report
IT	Information Technology
ITL	Information Technology Laboratory
LAN	Local Area Network
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OS	Operating System
OVAL	Open Vulnerability and Assessment Language
PDF	Portable Document Format
RFC	Request for Comment
U.S.	United States
XML	Extensible Markup Language