

Welcome to the latest edition of the OVAL-Announce e-newsletter. This email newsletter is designed to bring recent news about OVAL, such as OVAL data and schema updates, new Web site features, upcoming conferences, OVAL in the news, etc. right to your mailbox. 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 to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of assessment: 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. MITRE maintains OVAL and manages the OVAL Board and Community participation mail lists. Details on subscribing (and unsubscribing) to the email newsletter are at the end. Please feel free to pass this newsletter on to interested colleagues.

Comments: oval@mitre.org

OVAL-Announce e-newsletter/July 3, 2007

1. Feature Story
2. HOT TOPIC
3. Repository Updates Summary
4. Also In This Issue
5. Details/Credits + Subscribing and Unsubscribing

FEATURE STORY:

Version 5.3 of OVAL Now Available

Version 5.3 of OVAL has been moved to the "Official" stage and is now available on the OVAL Language Releases page. The OVAL Interpreter, Interpreter Source Code, and Data Files have also been updated.

Version 5.3 is a minor version change and includes the following: added sql test to the independent schema; changed the datatype of the comment attribute to not accept empty strings; added include_group and

resolve_group behaviors to the windows accesstoken_object; modified the schematron of the rpminfo_state to allow 'version' as a valid datatype for the and entities; added new privileges to the windows accesstoken_test; added an optional mask attribute; fixed a schema error that had a_time, c_time, and m_time defined as strings, changed to ints; added the audit event policy subcategories test to the windows schema; added a schematron rule in certain places to validate that an int value was supplied when a datatype of int was declared; added a share permission test to the windows schema; added a printer effective rights test; changed the trustee_name entity to trustee_sid for existing effective rights and audit permission tests, deprecated the original tests; added a check_existence attribute to and OVAL Test; added the 'none satisfy' value to the existing check attribute of an OVAL Test; added a ONE operator to the criterion element; added a user access control test; modified the hp-ux patch test; and updated the documentation. This minor version change Version 5.3 will not invalidate existing content that currently validates against Version 5.2. See the OVAL Language Releases page for more information.

The following have been updated to Version 5.3:

- * OVAL Definition schema
- * OVAL System Characteristics schema
- * OVAL Results schema

The following are also available for using Version 5.3:

- * OVAL Interpreter
- * Interpreter Source Code
- * Data Files
- * Bulk Content Download

The previous versions of the OVAL schemas, definitions, OVAL Interpreter, Interpreter source code, and data files have been archived. Visit the OVAL Language Releases page for the latest information on Version 5.3.

LINKS:

OVAL Language - <http://oval.mitre.org/language/index.html>

OVAL Interpreter - <http://oval.mitre.org/language/download/interpreter/index.html>

HOT TOPIC:

OVAL Mentioned in Article about Security Content Automation Protocol in "Government Computer News"

OVAL was mentioned in a May 22, 2007 article entitled "NIST releases FISMA security control tools" in "Government Computer News." The main topic of the article is the U.S. National Institute of Standards and Technology's (NIST) Security Content Automation Protocol (SCAP), which according to the article is an "automated checklist that uses a collection of recognized standards for naming software flaws and configuration problems in specific products. It can help test for the presence of vulnerabilities and rank them according to severity of impact. The checklist files are mapped to NIST specifications for compliance with the Federal Information Security Management Act, so that the output can be used to document FISMA compliance."

OVAL is mentioned when the author states that "SCAP currently uses six open standards for enumerating, evaluating and measuring the impact of software problems and reporting the results," and includes OVAL as follows: "Open Vulnerability and Assessment Language, OVAL, from MITRE; a standard XML for security testing procedures and reporting." The other five standards are: Common Vulnerabilities and Exposures (CVE), a dictionary of standard identifiers for security vulnerabilities related to software flaws; Common Configuration Enumeration (CCE), standard identifiers and a dictionary for system security configuration issues; Common Platform Enumeration (CPE), standard identifiers and a dictionary for platform and product naming; Extensible Configuration Checklist Description Format (XCCDF), a standard for specifying checklists and reporting results; and Common Vulnerability Scoring System (CVSS), a standard for conveying and scoring the impact of vulnerabilities.

SCAP is an expansion of the U.S. National Vulnerability Database (NVD) that is based upon the CVE List, and NVD, CVE, and OVAL are all sponsored by the National Cyber Security Division of the U.S. Department of Homeland Security.

LINK:

"NIST releases FISMA security control tools" article -
http://www.gcn.com/online/vol1_no1/44331-1.html?topic=security

REPOSITORY UPDATES SUMMARY

The OVAL Repository was updated since the last issue of Announce with 3 New Definitions, 2 Definitions with Status Changes, and 18 Modified Definitions. As of July 2, 2007 at 11:57 p.m. there are 2,024 total OVAL Definitions posted on the site. Of these, 1,495 are for Windows and 529 for UNIX.

Detailed information is available on the Latest Repository Updates page on the OVAL Web site, and by subscribing to our OVAL Repository RSS feed.

LINKS:

Latest Repository Updates - <http://oval.mitre.org/repository/data/Update.update>

OVAL RSS Feeds page - http://oval.mitre.org/news/rss_feeds.html

OVAL Repository main page - <http://oval.mitre.org/repository/index.html>

ALSO IN THIS ISSUE:

- * OVAL Interpreter Updated for Version 5.3
- * OVAL Repository Surpasses 2,000+ Definitions Milestone
- * "Guidelines for Submitting OVAL Definitions" Updated

Read these stories and more news at <http://oval.mitre.org/news/>

DETAILS/CREDITS + SUBSCRIBING AND UNSUBSCRIBING

Managing Editor: Jon Baker, Information Security Technical Center.

Writer: Bob Roberge. The MITRE Corporation (www.mitre.org) maintains OVAL and provides impartial technical guidance to the OVAL Community Forums and OVAL Board on all matters related to ongoing development of OVAL.

To unsubscribe from the OVAL-Announce e-newsletter, open a new email message and copy the following text to the BODY of the message "SIGNOFF OVAL-Announce-list", then send the message to: listserv@lists.mitre.org. To subscribe, send an email message to listserv@lists.mitre.org with the following text in the BODY of the message: "SUBSCRIBE OVAL-Announce-List".

Copyright 2007, The MITRE Corporation. OVAL and the OVAL logo are trademarks of The MITRE Corporation.

Information about the Common Vulnerabilities and Exposures (CVE) dictionary can be found at <http://cve.mitre.org>. For more information about OVAL, visit the OVAL Web site at <http://oval.mitre.org> or send an email to oval@mitre.org.