ITL BULLETIN FOR MARCH 2016

UPDATES TO THE NIST SCAP VALIDATION PROGRAM AND ASSOCIATED TEST REQUIREMENTS

Melanie Cook, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

NIST's Information Technology Laboratory has released the fourth revision of NIST Internal Report (NISTIR) 7511, *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*. SCAP 1.2 consists of a suite of specifications for standardizing the way security software communicates information about software flaws and security configurations.[2] The standardization of security information facilitates interoperability among products. It also enables disparate SCAP-enabled security software to provide consistent and predictable results. The SCAP Validation Program offers vendors an opportunity to provide independent verification that security software correctly processes SCAP-expressed security information and provides standardized output. Industry and government end users benefit from the SCAP Validation Program by having assurance that SCAP-validated products have undergone independent testing and have met all requirements defined in NISTIR 7511.

The validation program supports the U.S. Office of Management and Budget (OMB) efforts to provide consistent information technology configuration throughout the U.S. federal government. SCAP 1.2 is a key component of the legacy Federal Desktop Core Configuration (FDCC) program, which has now been replaced by the United States Government Configuration Baseline. OMB Memorandum M-08-22 to federal CIOs states that "both industry and government information technology providers must use SCAP-validated products with FDCC Scanner capability" to certify that: (i) "their products operate correctly with FDCC configurations"; and (ii) "do not alter FDCC settings."[3] While the FDCC Scanner capability has evolved and is now referred to as the Authenticated Configuration Scanner (ACS) capability, agencies continue to use SCAP products to confirm compliance with configuration requirements or identify deviations, as part of the Federal Information Security Management Act (FISMA) continuous monitoring components of an agency-wide information security program.

The SCAP Validation Program is supported by the NIST National Voluntary Laboratory Accreditation Program (NVLAP), under which various laboratories are accredited for performing independent test processes. NVLAP laboratories conduct the tests defined in the test requirements document (i.e., NISTIR 7511 Revision 4) on products and deliver the results to NIST. Based on the independent laboratory test

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.
[2] The SCAP 1.2 Specification is described in NIST SP 800-126 Revision 2.
[3] OMB Memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*, August 11, 2008, p. 2.

report, the SCAP Validation Program then validates the product under test. The validation certificates awarded to vendor's products are publicly posted on the NIST SCAP Validated Products website.

SCAP 1.2 Capabilities and Validations

Vendor products may seek validation for one core and two optional SCAP 1.2 capabilities on one or more platforms. The available capabilities consist of:

Authenticated Configuration Scanner (ACS)
An Authenticated Configuration Scanner has the capability to audit and assess a target system, using target system logon privileges and to determine its compliance with a defined set of configuration requirements. ACS may be combined with optional support for Common Vulnerabilities and Exposures (CVE) and/or Open Checklist Interactive Language (OCIL):

- ***CVE Option (optional CVE support may be combined with ACS)***
  The CVE option is the capability to support CVEs. This option may be awarded in conjunction with the ACS validation. The CVE option cannot be claimed by itself.

- ***OCIL Option (optional OCIL support may be combined with ACS)***
  The OCIL option is the capability to support the Open Checklist Interactive Language to collect information (data) from people and/or from existing data stores by other collection efforts. The OCIL option cannot be claimed by itself. This option may be claimed only in conjunction with the ACS capability.

NISTIR 7511 Revision 4 makes it easier for NIST to meet automation community needs by adding or removing platforms (e.g., operating systems) in future updates to the SCAP Validation Program. The platforms supported at the release of this document included several versions of Microsoft Windows and Red Hat Enterprise Linux. New platforms supported by the SCAP Validation Program will be listed on the SCAP Validation Program web page.

Updates in NISTIR 7511 Revision 4

NISTIR 7511 Revision 4 adds validation for SCAP-enabled software components, or modules. An SCAP module may be either a component of a product or a stand-alone product. The update adds an "SCAP 1.2 Inside" labeling program, with an SCAP 1.2 logo, for non-validated products that incorporate an SCAP-validated module. The new "SCAP 1.2 Inside" label and associated logo may be used by products that incorporate SCAP-validated modules after permission to use the logo has been granted by NIST. These marks do not imply product endorsement by NIST or the U.S. federal government, but they do help consumers to recognize non-validated products that incorporate an SCAP-validated module. "SCAP 1.2 Inside" products have not gone through the validation program testing process and will not be listed on the SCAP Validated Products web page. Only products that have successfully been awarded validation in accordance with the SCAP 1.2 specification and the NISTIR 7511 Revision 4 derived test requirements are listed on the SCAP Validated Products website.

NISTIR 7511 Revision 4 updated some test requirements and added several new ones, to further improve the overall reliability and consistency of SCAP results by validated products, and to assure that validated products comply with the SCAP specification. A *Summary of Changes* table in NISTIR 7511 Revision 4 provides a complete list of changes from Revision 3.

Guidance for Product Vendors and SCAP Product Consumers

Product vendors that wish to submit modules and/or software products for validation are encouraged to visit the SCAP Validation Program website to review the detailed requirements, accredited laboratory listings and other information.

Similarly, consumers who wish to acquire SCAP-enabled products will find listings of validated products at the same website, and a detailed "Frequently Asked Question" page that may be helpful.

Conclusion

NISTIR 7511 Revision 4 provides applicable test requirements for products that process SCAP 1.2 content and includes an improved set of tests that ensure consistent and reliable processing of such content. The list of currently supported platforms has been moved to an online location so that it may be expanded rapidly and updated quickly as both platforms and products evolve. To further enable this expanding set of SCAP-capable offerings, the program now includes validation of product modules in addition to turnkey product solutions.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov