ITL BULLETIN FOR SEPTEMBER 2010

SECURITY CONTENT AUTOMATION PROTOCOL (SCAP): HELPING ORGANIZATIONS MAINTAIN AND VERIFY THE SECURITY OF THEIR INFORMATION SYSTEMS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Managing the security of information systems is a challenging task for organizations. Many different and complex software components, including firmware, operating systems and applications, must be configured securely, patched when needed, and continuously monitored for security. Federal organizations must demonstrate compliance with mandated security requirements. Under the Federal Information Security Management Act (FISMA) of 2002, Title III of the E-Government Act (Public Law 107-347), federal organizations must report annually to the Congress and to the Office of Management and Budget (OMB) on the adequacy and effectiveness of their information security policies, procedures, and practices.

In the past, fulfilling these responsibilities has been time-consuming and error-prone because there have been no standardized, automated ways of performing the numerous tasks and reporting on the results. Another obstacle has been the lack of interoperability across security tools. For example, the use of proprietary names for vulnerabilities or platforms creates inconsistencies in reports from multiple tools, and this incompatibility can cause organizational delays in carrying out security assessments, decision-making, and vulnerability remediation activities.

The Security Content Automation Protocol (SCAP) was developed to overcome these deficiencies. Pronounced “ess-cap,” SCAP is a suite of specifications that standardize the format and nomenclature by which security software products communicate information about software identification, software flaws, and security configurations. A multipurpose protocol, SCAP supports automated vulnerability checking, technical control compliance activities, and security measurement. The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently issued a new publication to assist organizations in adopting and using SCAP.

NIST Special Publication (SP) 800-117, *Guide To Adopting and Using the Security Content Automation Protocol (SCAP), Version 1.0: Recommendations of the National Institute of Standards and Technology*

Written by Stephen Quinn, Karen Scarfone, and Chris Johnson of NIST, and by Matthew Barrett of G2, NIST SP 800-117 provides an overview of SCAP, explaining why it was created, the current components of SCAP, and the product validation and laboratory accreditation programs that support SCAP. One section of the publication presents NIST's recommendations for using SCAP to verify that technical security controls comply with requirements and to communicate information regarding vulnerabilities in a standardized manner. Another section advises information technology (IT) vendors how they can implement SCAP Version 1.0 capabilities within their products and services.

The appendices of NIST SP 800-117 contain detailed supporting information on how SCAP can be used to verify compliance with the security requirements of FISMA and how SCAP components can be used to automate the development of evidence of compliance with the technical control requirements of FISMA. Also included in the appendices are lists of the acronyms and abbreviations used in the guide and SCAP-related resources available online.

NIST SP 800-117 is available from the NIST Web page http://csrc.nist.gov/publications/PubsSPs.html#800-117.

How SCAP Helps Organizations Manage Security and Comply With Reporting Requirements

SCAP was designed to organize, express, and measure security-related information in standardized ways. SCAP supports the use of standard reference data, such as identifiers for post-compilation software flaws and security configuration issues. SCAP can be used to maintain the security of enterprise systems by automatically verifying the installation of patches, checking system security configuration settings, and examining systems for signs of compromise.

General information about the SCAP program is available from the NIST Web page http://scap.nist.gov/.

Organizations must manage the security of many different systems, applications, and operating systems that have different mechanisms for patching and managing security configuration. The same software often needs to be secured somewhat differently on multiple hosts. Another issue is the need to reconfigure software or install patches when vulnerabilities are discovered and when systems are targeted by attackers. Priorities must be established to assure that the most important vulnerabilities are addressed quickly. When vulnerability scanners do not use standardized names for vulnerabilities, the security staff may be unsure whether the different scanners are reporting on the same vulnerabilities.

In complying with FISMA, federal organizations have to map the low-level technical details of their system security, such as individual security configuration settings, to high-level security requirements that are expressed in federal mandates and directives. Determining the mappings is time-consuming and is highly susceptible to errors and differences in interpretation. NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*, addresses this problem by organizing the required security controls for FISMA into 17 security control families and

117 controls. Many of these controls deal with how systems are configured, patched, and securely operated, but not all of the controls are at the lowest technical level and additional mappings to higher technical levels may be needed. NIST SP 800-53, Rev. 3, and supporting resources are available at http://csrc.nist.gov/publications/PubsSPs.html#800-53, https://web.nvd.nist.gov/view/800-53/home, and http://csrc.nist.gov/groups/SMA/fisma/support_tools.html.

The standardized, automated methods provided by SCAP enable organizations to manage these time-consuming and error-prone processes, and to overcome the lack of interoperability among different security tools. SCAP can be used to demonstrate compliance with the requirements established by FISMA, as well as other requirements: for example, INCITS/ISO/IEC 27001, an international standard specifying the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security management systems; Department of Defense (DOD) Directive 8500, establishing information assurance requirements; and the Federal Information System Controls Audit Manual (FISCAM). Individual specifications that comprise SCAP can also be used for forensic activities and other purposes.

SCAP does not replace existing security software, and support for SCAP can be incorporated into existing software.

The Technical Specifications for SCAP

NIST SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP*, defines the technical composition of SCAP Version 1.0. It describes six specifications and their interrelationships. The specifications are grouped into three categories: languages for specifying checklists, generating checklist reports, and specifying the low-level testing procedures used by the checklists; enumerations that include nomenclatures and dictionaries for security and product-related information; and vulnerability measurement and scoring systems for measuring the characteristics of vulnerabilities and generating scores based on those characteristics. The current specifications are:

· eXtensible Configuration Checklist Description Format (XCCDF), an Extensible Markup Language (XML) specification for structured collections of security configuration rules used by operating system (OS) and application platforms;

· Open Vulnerability and Assessment Language (OVAL™), an XML specification for exchanging technical details on how to check systems for security-related software flaws, configuration issues, and patches;

· Common Platform Enumeration (CPE™), a naming convention for hardware, OS, and application products;

· Common Configuration Enumeration (CCE™), a dictionary of names for software security configuration issues, such as access control settings, password policy settings;

· Common Vulnerabilities and Exposures (CVE™), a dictionary of names for publicly known security-related software flaws; and

· Common Vulnerability Scoring System (CVSS), a method for classifying characteristics of software flaws and assigning severity scores based on these characteristics.

(OVAL, CCE, CPE, and CVE are trademarks of The MITRE Corporation.
XCCDF and SCAP are trademarks of NIST.)

SCAP utilizes standard reference data to identify software flaws and security configurations. Also known as *SCAP content*, this reference data is provided by the National Vulnerability Database (NVD), which is managed by NIST and sponsored by the Department of Homeland Security (DHS). The National Vulnerability Database is available at http://nvd.nist.gov/.

NIST's Recommendations to Organizations for Adopting and Using SCAP

NIST recommends that organizations adopt the following practices to take advantage of the capabilities of SCAP to organize, express, and measure security-related information in standardized ways, and to use related reference data, such as identifiers for post-compilation software flaws and security configuration issues.

• Use security configuration checklists that are expressed using SCAP to improve and monitor the security of systems.

A security configuration checklist that is expressed using SCAP (an SCAP-expressed checklist) documents the desired security configuration settings, installed patches, and other system security elements in a standardized format. Organizations should identify and obtain SCAP-expressed checklists for their systems' software, then customize the checklists as appropriate to meet specific organizational requirements. After fully testing the checklists, organizations should implement their recommendations. While the current version of SCAP does not provide a capability to automatically implement checklists, SCAP-expressed checklists can be applied using proprietary methods. Organizations should use SCAP-expressed checklists on an ongoing basis to confirm that systems are configured properly. Federal agencies should use SCAP-expressed checklists to ensure conformance to NIST and OMB security configuration guidance.

Information about the National Checklist Program, a government repository of available security checklists, is available at http://checklists.nist.gov.

• Use SCAP to demonstrate compliance with high-level security requirements that originate from mandates, standards, and guidelines.

SCAP-expressed checklists can map individual system security configuration settings to their corresponding high-level security requirements. For example, NIST has added configuration identifiers for every security configuration settings to the Windows 7 Checklists. NIST then provides reference data mapping each security configuration setting to the high-level security controls described in NIST SP 800-53, Rev. 3. These mappings can help demonstrate that the implemented settings adhere to FISMA requirements. The configuration identifiers are embedded in SCAP-expressed checklists, which allow SCAP-enabled tools to automatically generate assessment and compliance evidence when combined with the mapping reference data. This increased automation can significantly reduce the effort needed to achieve assessment results, providing substantial cost savings. To produce evidence of compliance with FISMA for many of the security controls identified in NIST SP 800-53, Rev. 3, federal agencies should use SCAP-enabled tools along with SCAP-expressed checklists.

Information about the mapping of security configuration settings to the security controls is available at http://nvd.nist.gov/cce.cfm.

• Use standardized SCAP enumerations—identifiers and product names.

Organizations frequently use a collection of tools for security management, such as vulnerability scanners, patch management utilities, and intrusion detection systems. SCAP allows organizations to use standardized enumerations when referring to security-related software flaws, security configuration issues, and platforms. The common understanding achieved through the use of standardized enumerations makes it easier to use security tools, share information, and provide guidance to address security issues. Organizations should encourage security software vendors to incorporate support for Common Vulnerabilities and Exposures (CVE), Common Configuration Enumeration (CCE), and Common Platform Enumeration (CPE) into their products. All software vendors should be encouraged to include CVE and CCE identifiers and CPE product names in their vulnerability and patch advisories.

• Use SCAP for vulnerability measurement and scoring.

SCAP enables quantitative and repeatable measurement and scoring of software flaw vulnerabilities across systems through the combination of the Common Vulnerability Scoring System (CVSS), CVE, and CPE. The ability to accurately and consistently convey the characteristics of a vulnerability allows organizations to institute consistent and repeatable mitigation policies throughout the enterprise. Organizations should use CVSS base scores to assist in prioritizing the remediation of known security-related software flaws based on the relative severity of the flaws. CVSS scores can be used more easily when organizations use CVE to reference specific vulnerabilities whenever possible. When a new vulnerability is publicly announced, a new CVE identifier is created for it, the affected products are identified using CPE, and the CVSS base measures and score are computed and added to the National Vulnerability Database. Organizations can review the CVSS base measures and scores for each new CVE as part of their processes to prioritize and mitigate vulnerabilities. SCAP content can be used to check systems for the presence of the new vulnerability.

• **Acquire and use SCAP-validated products.**

NIST has established an SCAP product validation program to ensure that SCAP products are thoroughly tested and validated to conform to SCAP requirements. The validation program emphasizes a modular component architecture such that SCAP-validated products are interoperable and interchangeable. The validation program also focuses on correctness testing where appropriate, such as for vulnerability and configuration scanning. Many acquisition officials have included requirements for SCAP-validated products in their procurements. For example, OMB requires federal agencies and agency IT providers to use SCAP-validated Federal Desktop Core Configuration (FDCC) scanners for testing and assessing FDCC compliance. See the following Web page for information about the FDCC: http://fdcc.nist.gov/.

• **Software developers and checklist producers should adopt SCAP and use its capabilities.**

Software developers should ensure that their software products are capable of assessing the underlying software configuration settings using SCAP, rather than relying on manual checks or proprietary checking mechanisms. Also, product vendors and other checklist developers should create their checklists using SCAP. NIST encourages IT product vendors to participate in SCAP content development because of their depth of knowledge and their ability to speak authoritatively about the most effective and accurate means of assessing the security configurations of their products. Checklist developers are urged to contribute their applicable security configuration checklists to NIST's National Checklist Program to promote the widespread availability of the checklists.

The SCAP Validation Program

NIST developed the SCAP Validation Program to test products for the capability to use the features and functionality available through SCAP.

Under the SCAP Validation Program, independent laboratories are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP). These laboratories conduct defined tests on information system security products and submit a test report and relevant results to NIST. Based on the independent laboratory's test report, the SCAP Validation Program then validates the product under test. A list of validated products is publicly available.

SCAP validation focuses on evaluating specific versions of vendor products based on the platforms they support. Validations are awarded on a platform-by-platform basis for the version of the product that was validated. Currently, the validation program focuses on evaluating and validating SCAP implementations for Windows operating systems.

Information about the SCAP Validation Program is available at http://scap.nist.gov/validation/.

The SCAP Validation Program Derived Test Requirements are available at http://csrc.nist.gov/publications/drafts/nistir-7511/Draft-NISTIR-7511r2.pdf.

The list of SCAP Validated Tools is available at http://nvd.nist.gov/scapproducts.cfm.

Ongoing Activities to Support the Development of SCAP

NIST plans to add specifications to SCAP to provide standardized methods for automated implementation of checklists. Also, NIST plans to validate SCAP products for platforms in addition to the Windows operating systems. See the following NIST Web page for details: http://scap.nist.gov/emerging-specs/listing.html.

NIST is revising SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Revision 1*, to define SCAP Version 1.1 in terms of both its component specifications and the requirements for SCAP content, and to describe the details of how the elements of SCAP interoperate. The revision focuses on the requirements and conventions that are to be employed to ensure the consistent and accurate exchange of SCAP content and the ability to reliably use the content with SCAP validated products.

See the following NIST Web page for more details: http://csrc.nist.gov/publications/PubsSPs.html#800-126-r1.

NIST has developed three draft Interagency Reports (NISTIRs) on Common Platform Enumeration (CPE), which provides a standardized way to identify and describe software and hardware devices that an organization operates. The three draft reports propose specifications to be issued as part of CPE version 2.3:

> NISTIR 7695, Draft *Common Platform Enumeration: Naming Specification Version 2.3*, defines the CPE naming specification, including the logical structure of well-formed CPE names and the procedures for binding and unbinding these names with machine-readable encodings.
>
> NISTIR 7696, Draft *Common Platform Enumeration: Name Matching Specification Version 2.3*, provides the CPE matching specification, which defines procedures for comparing CPE names to determine whether they refer to some or all of the same products or platforms.

> NISTIR 7697, Draft *Common Platform Enumeration: Dictionary Specification Version 2.3*, contains the CPE dictionary specification, which defines the concept of a dictionary of identifiers and prescribes high-level rules for dictionary curators.

Another draft publication, NISTIR 7669, *Open Vulnerability Assessment Language (OVAL) Validation Program Derived Test Requirements*, describes the requirements for products for OVAL Validation under the NIST NVLAP.

These reports are available from the NIST Web page http://csrc.nist.gov/publications/PubsNISTIRs.html.

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.