**NIST Special Publication 800-117**

NIST Publications

Provides an overview of Security Content Automation Protocol (SCAP), focusing on how organizations can use SCAP-enabled tools to enhance their security. It also explains to IT product and service vendors how they can adopt SCAP (http://scap.nist.gov). SCAP is more-or-less the combination of some enumerations (CCE, CPE, CVE), a scoring system (CVSS), and some XML languages (XCCDF, OVAL).

**NIST Special Publication 800-126**

This is the Technical Specification for SCAP, focusing on how software developers can integrate SCAP technology into their products.

**NIST Interagency Report 7511**

Describes the requirements that must be met by products to achieve SCAP validation. Validation is awarded based on a defined set of SCAP capabilities by independent laboratories that have been accredited for SCAP testing by NIST. IR 7511 has been written primarily for accredited laboratories and for vendors interested in receiving SCAP validation for their products.

**Common Configuration Enumeration (CCE)**

CCE assigns identifier tags to each commonly recognized configuration issue. These identifiers are intended to be unique tags or keys, not descriptive names. CCE entries contain a humanly understandable description of the configuration issue; for example, a valid CCE description might be "The minimum password length should be set appropriately". CCE is a part of SCAP and maintained by MITRE.

Enumerations

**Common Platform Enumeration (CPE)**

CPE is a naming scheme for IT systems and software packages to clearly identify the IT platforms to which vulnerabilities apply.

**Common Vulnerabilities and Exposures (CVE)**

CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal is to make it easier to share data across separate tools, repositories and services with this common ID naming system.

Metrics

**Common Vulnerability Scoring System (CVSS)**

CVSS is a formula for computing the severity and urgency of a vulnerability in a way which is platform- and vendor-neutral. CVSS severity rankings help to prioritize security remediation work. It is currently maintained by FIRST (www.first.org), not NIST or MITRE.

Languages

**eXtensible Configuration Checklist Description Format (XCCDF)**

XCCDF is an XML specification for writing security checklists, benchmarks and related kinds of documents, and also defines a data model and format for storing results of benchmark compliance testing. XCCDF is a part of SCAP, it is maintained by NSA and NIST.

**Open Vulnerability and Assessment Language (OVAL)**

OVAL is a language to express checks for determining whether software vulnerabilities exist on a system to provide consistent and reproducible metrics. OVAL uses the public vulnerabilities identified in CVE as the basis for most of the OVAL vulnerability definitions.

**Asset Reporting Format (ARF)** -- Emerging Specification Not In SCAP Yet

ARF is a format for exporting detailed, per-device assessment data between network assessment tools. ARF is intended to be used by vulnerability scanners, XCCDF scanners, and other tools that collect detailed configuration data about networked devices.

Emerging Specifications

**Common Configuration Scoring System (CCSS)** -- Emerging Specification Not In SCAP Yet

CCSS is a set of standardized measures for the characteristics and impacts of different types of vulnerabilities. CCSS data can assist organizations prioritize security remediation work. See NIST Interagency Report 7502.

**Common Misuse Scoring System (CMSS)** -- Emerging Specification Not In SCAP Yet

CMSS is a set of standardized measures for vulnerabilities stemming from software feature misuse. CMSS data can be used along with CVSS and CCSS data to assist organizations in prioritizing security remediation work. See NIST Interagency Report 7517.

**Open Checklist Interactive Language (OCIL)** -- Emerging Specification Not In SCAP Yet

OCIL defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions, such as for security checklists.

**Open Checklist Reporting Language (OCRL)** -- Emerging Specification Not In SCAP Yet

OCRL is a language for XML definitions that gather information from systems and present it as a standardized report for human evaluation of policy compliance, but only for when a human or human judgment is necessary to determine compliance.