Security Content Automation Protocol (SCAP)

SCAP Vendor Assertions Document

July 20, 2016

by

SPAWARSYSCEN Atlantic: Charleston
P. O. Box 190022
North Charleston, SC 29419-9022

http://www.public.navy.mil/spawar/Atlantic/ProductsServices/Pages/SCAP.aspx

For

SCAP Compliance Checker

Version 4.1.1, CPE cpe:/a:spawar:scap_compliance_checker:4.1.1

Assertion:

SPAWAR asserts that SCAP Compliance Checker version 4.1.1 meets or exceeds the Derived Test Requirements (DTR) for SCAP 1.2 as described in NIST IR 7511, Revision 4, for the following SCAP capabilities and supported platforms:

Capabilities:

- ☑ Authenticated Configuration Scanner
- ☑ CVE
- ☑ OCIL

Platforms:

- ☑ Microsoft Windows XP Pro SP 3
- ☑ Microsoft Windows Vista SP
- ☑ Microsoft Windows 7 SP _ 32-bit
- ☑ Microsoft Windows 7 SP_ 64-bit*
- ☑ Microsoft Windows 8.1 SP_ 32-bit
- ☑ Microsoft Windows 8.1 SP_ 64-bit
- ☑ Microsoft Windows Server 2012 R2 SP_ 64-bit*

- ☑ Red Hat Enterprise Linux 5 32 bit
- ☑ Red Hat Enterprise Linux 5 64 bit
- ☑ Red Hat Enterprise Linux 6 32 bit*
- ☑ Red Hat Enterprise Linux 6 64 bit
- ☑ Red Hat Enterprise Linux 7 32 bit
- ☑ Red Hat Enterprise Linux 7 64 bit*

* indicates platform that SCAP 1.2 validation was officially performed on.

SCAP Component Technologies:

The following table provides a brief summary of the individual SCAP Component Standards supported by SCAP Compliance Checker:

Supported	Component	Version	Description
☑	AI	1.1	Asset Identification (AI) is a specification for identifying assets
☑	ARF	1.1	The Asset Reporting Format (ARF) is a specification describing a data model for asset reporting
☑	CCE	5	The Common Configuration Enumeration ™ (CCE) is a nomenclature and dictionary of software security configurations
☑	CCSS	1.0	The Common Configuration Scoring System (CCSS) is a specification for measuring the relative severity of system security configuration issues
☑	CPE	2.3	The Common Platform Enumeration (CPE) is a specification measuring the relative severity of system security configuration issues
☑	CVE	n/a	The Common Vulnerability Enumeration® (CVE) is a specification describing a nomenclature and dictionary of security-related software flaws
❑	CVSS	2.0	The Common Vulnerability Scoring System is a language for representing system configuration information, assessing machine state, and reporting assessment results
☑	OCIL	2.0	The Open Checklist Interactive Language (OCIL) is a language for

			representing checks that collect information from people or from existing data stores made by other data collection efforts
☑	OVAL	5.10.1	The Open Vulnerability and Assessment Language is a language for representing system configuration information, assessing machine state, and reporting assessment results
☑	SCAP	1.2	SCAP is a specification for expressing and manipulating security data in standardized ways. SCAP uses several individual specifications in concert to automate continuous monitoring, vulnerability management, and security policy compliance evaluation reporting
☑	TMSAD	1.0	The trust Model for Security Automation Data (TMSAD) describes a common trust model that can be applied to specifications within the security automation domain
☑	XCCDF	1.2	Extensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents

SCAP Implementation Statement(s):

The SCAP Compliance Checker (SCC) processes SCAP content with full support for the SCAP 1.0, 1.1, and 1.2 specifications.

SCC parses requirements from SCAP content streams which are composed of ARF, XCCDF, OVAL, OCIL, and CPE Dictionary XML documents. It then, surveys target systems for compliance with those requirements and produces detailed results in valid XML, HTML, and text formats. The detailed reports enable system administrators to efficiently bring their systems into compliance.

SCC performs XML schema validation on both input (SCAP content streams) and output XML files.

SCC performs digital signature validation (when a signature exists within SCAP 1.2 content) using the TMSAD specification, and verifies that the content was signed using a known and trusted digital certificate.

SCC supports OVAL 5.11.1 and many other OVAL tests not required by SCAP 1.2. It also supports many operating systems not officially part of SCAP 1.2, including Solaris, Mac OS X, HP-UX, AIX and Debian Linux.

For more information, please refer to our product page:
http://www.public.navy.mil/spawar/Atlantic/ProductsServices/Pages/SCAP.aspx

SCAP Backwards Compatibility:

SCC is fully backward compatible with SCAP version 1.1 with XCCDF version 1.1.4; OVAL versions 5.3, 5.4, 5.5, 5.6, 5.7, and 5.8; and OCIL version 2.0. The SCC is also fully backward compatible with SCAP 1.0 with XCCDF version 1.1.4 and OVAL versions 5.3 and 5.4.

From and end-user's perspective, the SCC command line and graphical user interface operate in the same general manner for SCAP 1.2, 1.1, and 1.0 content streams. The primary difference is during content installation, where with SCAP 1.2 streams SCC supports selecting a single XML datastream to install the content, with SCAP 1.1 and 1.0 content, the collection of XML content files must be zipped prior to installation.

When SCAP 1.2 content is used, SCC creates ARF, XCCDF, OVAL and OCIL XML results.
When SCAP 1.1 content is used, SCC creates XCCDF, OVAL and OCIL XML results.
When using SCAP 1.0 content, SCC creates XCCDF and OVAL results.

Disclaimer:

This information is provided in good faith and is believed to be true and accurate.