

## Security Content Automation Protocol (SCAP)

SCAP Vendor Assertions Document v3.3

10/23/2013

by:



**Tripwire, Inc.**

**101 SW Main Street, Suite 1500**

**Portland, OR 97204**

For



**Tripwire Enterprise**

**Version 8**

**cpe:/a:tripwire:tripwire\_enterprise:8.3**

**cpe:/a:tripwire:twoval\_plug-in:1.0.0**

**cpe:/a:tripwire:via\_agent:2.2.0**

### **Assertion:**

Tripwire, Inc. asserts that Tripwire Enterprise version 8 meets or exceeds the Derived Test Requirements (DTR) for SCAP 1.2 as described in NIST IR 7511 Revision 3 January 2013 Update for the following SCAP capabilities and supported platform family:

**Capabilities:**  Authenticated Configuration Scanner

CVE

**Platforms:**  Microsoft Windows 7 SP\_ 32-bit

Microsoft Windows 7 SP\_ 64-bit

Red Hat Enterprise Linux 5 Desktop 32 bit

Red Hat Enterprise Linux 5 Desktop 64 bit

### SCAP Component Technologies:

The following table provides a brief summary of the individual SCAP Component Standards supported by Tripwire Enterprise version 8:

Supported	Component	Version	Description
[X]	AI	[ 1.1 ]	Asset Identification (AI) is a specification for identifying assets
[X]	ARF	[ 1.1 ]	The Asset Reporting Format (ARF) is a specification describing a data model for asset reporting
[X]	CCE	[ 5 ]	The Common Configuration Enumeration™ (CCE) is a nomenclature and dictionary of software security configurations
[X]	CCSS	[ 1.0 ]	The Common Configuration Scoring System (CCSS) is a specification for measuring the relative severity of system security configuration issues
[X]	CPE	[ 2.3 ]	The Common Platform Enumeration (CPE) is a specification measuring the relative severity of system security configuration issues
[X]	CVE	[ n/a ]	The Common Vulnerability Enumeration® (CVE) is a specification describing a nomenclature and dictionary of security-related software flaws
[X]	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
[X]	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
[X]	SCAP	[ 1.2 ]	SCAP is a specification for expressing and manipulating security data in a 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.
[X]	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):

**Tripwire Enterprise Console** software is installed on a single system, known as the **Tripwire Enterprise Server**. When working with SCAP-based content, users interact with the Security Content Processor (SCP) component of Tripwire Enterprise using a REST API. The SCP imports SCAP-based content and derives OVAL definitions and tests from it, then sends them to Tripwire VIA Agents. The Agents execute the OVAL tests to gather system characteristics from monitored endpoints, then return the system characteristics to the TE Console where they are evaluated to produce results.

**Tripwire VIA Agent** software is a lightweight agent installed on each system to be monitored. A VIA Agent harvests system characteristics from a monitored endpoint and returns them to the TE

Console for evaluation. All communication between the VIA Agent and the TE Server is secured using SSL.

**SCAP Backwards Compatibility:** Tripwire Enterprise, version 8, supports SCAP content versions 1.0, 1.1 and 1.2 that includes the corresponding versions of OVAL and XCCDF that were cited by those versions of SCAP.

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

Copyright © 2013 Tripwire, Inc. All Rights Reserved