**Security Content Automation Protocol (SCAP)**

SCAP Vendor Assertions Document v3.6

9 June, 2016

*By*

****

**ThreatGuard, Inc.**

**1100 NW Loop 410**

**Suite 700**

**San Antonio, TX**

**78213**

**https://www.ThreatGuard.com**

*For*

****

**Secutor Compliance Automation Toolkit (S-CAT)**

**Version 5, CPE cpe:/a:threatguard:s-cat:5**

**Assertion:**

ThreatGuard, Inc. asserts that S-CAT, version 5 meets or exceeds the Derived Test Requirements (DTR) for SCAP 1.2 as described in NIST IR 7511, Revision 4, Update <Update Number> for the following SCAP capabilities and supported platform family:

|  |  |  |
| --- | --- | --- |
| **Capabilities:** |  | Authenticated Configuration Scanner |
|  |  | CVE |
|  |  | OCIL |
|  |  |  |
| **Platform Family:** |  | Windows XP Professional SP3 (32 bit edition) |
|  |  | Windows Vista SP2 (32 bit edition) |
|  |  | Windows 7 SP1 (32 bit edition) |
|  |  | Windows 7 SP1 (64 bit edition) |
|  |  | Windows 8.1 (32 bit edition) |
|  |  | Windows 8.1 (64 bit edition) |
|  |  | Windows Server 2012 R2 (64 bit edition) |
|  |  | Red Hat Enterprise Linux 5 Desktop (32 bit edition) |
|  |  | Red Hat Enterprise Linux 5 Desktop (64 bit edition) |
|  |  | Red Hat Enterprise Linux 6 Desktop (32 bit edition) |
|  |  | Red Hat Enterprise Linux 6 Desktop (64 bit edition) |
|  |  | Red Hat Enterprise Linux 7 Desktop (32 bit edition) |
|  |  | Red Hat Enterprise Linux 7 Desktop (64 bit edition) |

**SCAP Component Technologies:**

The following table provides a brief summary of the individual SCAP Component Standards supported by S-CAT:

|  |  |  |  |
| --- | --- | --- | --- |
| **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 TM (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):**

|  |
| --- |
| S-CAT is a suite of tools used to add SCAP and OVAL capabilities to other products and is used as the standards engine for ThreatGuard desktop and enterprise compliance management tools (Prime and Magnus, respectively). S-CAT is the engine that powers compliance for other industry-leading products.  Some key features of the S-CAT suite of tools:   * Multiple integration paths * Coverage for all validation target types and many others * Support both local and remote (agentless) assessments * Ability to account for deviations from policy * Automated remediation: system changes are driven by the assessment content |

**S-CAT Versioning:**

|  |
| --- |
| S-CAT uses a single release number to simplify mapping version number to the level of SCAP compliance.  For SCAP 1.2, the S-CAT release is "5".  If necessary, updates are released to address bug fixes and maintain the strictest adherence to SCAP compliance and individual update releases can be identified by the internal library build number which can be printed via the command line using the '-v' option.  Update details are available in the **ReleaseNotes.txt** document included with each update bundle.  The library build number uses a version format of “M.m.t.b” where  M = Major  m = minor  t = tiny  b = build  A change in the Major number indicates a significant revision to the library. All efforts are made to maintain backward compatibility, but this is not guaranteed with a release that changes the major revision number. The Major number will be kept in sync with the version number of other products to avoid confusion and thus is typically an indicator of which SCAP release is being supported.  A change to the minor number indicates that small changes have been made.  A change to the tiny number indicates that very small changes have been made that have little to no effect on functionality, such as correcting typos, changes to output format, and so on.  The build number is incremented as part of the full build process. Since the build process can be triggered by other software products that rely on the library this number can often change even if there are no software changes to the library itself. |

**SCAP Backwards Compatibility:**

|  |
| --- |
| S-CAT is able to detect older versions of SCAP content and process it in accordance with the previous specifications. |

**Disclaimer:**

|  |
| --- |
| This information is provided in good faith and is believed to be true and accurate.  <Copyright © 2016 ThreatGuard, Inc. All Rights Reserved> |