SAINT Implementation Statements

Security Content Automation Protocol (SCAP) Compliance Test Submission

July 18, 2014

Submitted by:
SAINT Corporation
4720 Montgomery Lane, Suite 800
Bethesda, MD 20814
(800) 596-2006
www.saintcorporation.com

Table of Contents

Purpose.....3
SAINT Implementation Statements 4

Purpose

The purpose of this document is to submit SAINT Corporation's Implementation Statements applicable to the following Security Content Automation Protocol (SCAP) capabilities specified under SCAP v.1.2 standards:

- Authenticated Configuration Scanner (ACS) and
- Common Vulnerabilities and Exposures (CVE)

SAINT Corporation submits its flagship product, SAINT 8 Security Suite, for validation and acknowledges that this product will support all Windows and Linux platforms that are included as part of the SCAP Validation Program, specifically:

- Microsoft Windows XP Professional with Service Pack 3
- Microsoft Windows Vista with Service Pack 2
- Microsoft Windows 7, 32- and 64-bit
- Red Hat Enterprise Linux 5 Desktop, 32- and 64-bit

These capabilities include the following SCAP components:

- eXtensible Configuration Checklist Description Format (XCCDF)
- Open Vulnerability and Assessment Language (OVAL™)
- Common Configuration Enumeration (CCE™)
- Common Platform Enumeration (CPE™)
- Common Vulnerabilities and Exposures (CVE®)
- Common Vulnerability Scoring System (CVSS)
- Asset Identification (AI)
- Asset Reporting Format (ARF)
- Trust Model for Security Automation Data (TMSAD)

This document is one of two deliverables required for this process. Also reference SAINT Corporation's deliverable document "Required Vendor Information", dated July 18, 2014 for details related to this submission.

SAINT Implementation Statements

SCAP

SAINT 8 Security Suite provides support to the Security Content Automation Protocol (SCAP) specification as an Authenticated Configuration Scanner (ACS), including the Common Vulnerabilities and Exposures (CVE) option. SAINT 8 provides support to SCAP requirements defined for each of these components, as defined in SP 800-126, Revision 2, the SCAP specification, and verified by compliance testing against the Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements (NISTIR 7511, Revision 3), dated January 2013 – including updates as of July 2013.

SAINT 8 Security Suite is the major release from SAINT Corporation submitted to a NIST-approved test lab for validation with the SCAP Version 1.2 standards. SAINT 8's release strategy includes a numbering convention that delivers periodic feature releases (8.x) and security content (8.x.x) that offer added capabilities and functionality since the 8.0 launch in 2013. SAINT 8's version 8.4 was the tested version in 2014 and validates SAINT 8 compliance with the SCAP v.1.2 standard as of SAINT 8.4 and above.

SAINT 8 provides support for open standards languages, enumerations and metrics that currently include XCCDF, OVAL, CCE, CPE, CVE and CVSS, AI, ARF and TMSAD of the specification. SAINT 8 also provides support for the U.S. Government Configuration Baseline (USGCB) by ingesting valid SCAP-expressed data streams and assessing target configurations against these baselines. This capability also includes support for evaluating SCAP content to scan for compliance, vulnerabilities, and patches using both standalone OVAL definition files and OVAL definitions contained in SCAP-expressed data streams.

SAINT 8 completes this capability by providing data analysis, links to external authoritative sources of information, policy editing and reporting interfaces, to facilitate local policy investigation and analysis. Compliance reporting is provided via pre-defined report templates and custom presentation of output in machine-readable and many human-readable formats, such as HTML, PDF, XML and CSV.

USGCB

SAINT Corporation asserts that the SAINT 8 Security Suite is fully functional and operates correctly as intended on systems using the U.S. Government Configuration Benchmark (USGCB). Target settings applicable to performing USGCB assessments are defined in the SCAP section the *SAINT 8 User Guide*. To run a scan, the targets must meet only the requirements for running a normal SAINT 8 authenticated scan. Targets can be scanned for USGCB compliance by importing the desired USGCB SCAP Data Stream containing XCCDF and OVAL document formats, and selecting it when choosing a scan policy to run. USGCB scans make use of CCE to simply tracking of configuration issues found during a scan. SAINT 8 produces multiple reports in both the required formats for SCAP and some non-required formats for data analysis. The reports are viewable in the *SCAP Data* section of the GUI and can also be bundled and downloaded to support external requirements such as content backups, compliance reporting or importing into other applications.

XCCDF

XCCDF (eXtensible Common Configuration Data Format) is a specification language for writing security checklists, benchmarks and related types of documents, as defined by NIST. SAINT 8 provides the capability to import, validate, view, execute policy scans, and report on benchmarks in XCCDF format, Version 1.2. SAINT 8 provides two methods of collection: 1) Select a supported policy to validate and Import or Update content; and 2) Use the *Upload Benchmark* option in the SCAP data grid to manually import definitions for validation and execution by SAINT's scanning engine. This capability includes support for importing SCAP expressed data-streams in ZIP and XML formats.

SAINT 8 also provides a Policy Editor for those users that wish to use an existing XCCDF-based policy as a template to edit and save a custom policy to support local requirements. This editor allows users to view such information as the detailed descriptions of each group and rule contained in a policy; and to enable checks, disable checks (rules) and modify values associated with certain rules.

XCCDF-based scan results can be viewed or downloaded in a number of compliance formats: XCCDF Results document; XCCDF Human readable results document; OVAL system characteristics for each target; and OVAL Results documents that resulted from the XCCDF scan.

OVAL

Open Vulnerability and Assessment Language (OVAL) is an international information security standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. SAINT 8 supports OVAL definitions of the patch, vulnerability, compliance and inventory class for most platforms and adheres to the latest OVAL schema (e.g. v.5.10.1 as of the date of SCAP v.1.2 validation). The SAINT 8 scanning engine then consumes and executes selected definitions and assesses hosts, without the need for a local agent or plug-in, to determine and report issues found on the hosts.

SAINT 8 supports OVAL compliance checking by allowing users to import OVAL checks (standalone and/or SCAP-expressed data streams) from the OVAL repository, as well as importing user-developed XML files containing OVAL checks. An SCAP-expressed data stream is defined as “a collection of four or more related XML files containing SCAP data using the SCAP components that provide the data necessary to evaluate systems for compliance with a configuration-based security policy”. SAINT 8 also provides viewing and downloading OVAL result files via the GUI, as well as viewing human readable (non XML) results.

CCE

Common Configuration Enumeration (CCE) is a dictionary of names for software security configuration issues (e.g., access control settings, password policy settings). As such, CCEs describe system configuration issues to facilitate correlation of configuration data across multiple information sources and tools. SAINT 8 provides support for CCE’s by displaying CCE IDs, in accordance with the specifications and CCE 5.0 schema located on the *Mitre.org CCE website* for each configuration item in scanning results produced for XCCDF scanning policies and profiles. SAINT 8 also provides data drill-down and report configuration options that include displaying CCE ID and Descriptions. CCE IDs are displayed in several of the different reports offered via the *Data Analysis - SCAP Results* page. These include the required output format defined as “CCE ID, pass/fail” and a detail format which organizes results by XCCDF Rules, and displays results for each XCCDF Rule, to include: the CCE IDs; CCE descriptions; whether or not the CCE passed/failed against the target system; and why the CCE passed/failed against the target system. SAINT 8 provides a policy editor to allow users to disable and enable configuration checks by CCE to meet specific network requirements.

CPE

CPE (Common Platform Enumeration) is a structured naming scheme for information technology systems, software and packages. SAINT 8 provides support for CPE, version 2.3, by using the CPE names which are defined in the *official CPE dictionary* then mapping all known CVE(s) to the corresponding CPE(s) for a given year. SAINT 8 also facilitates CPE content updates directly from the authoritative source, as a product feature, to remove the burden of data maintenance from the user and to ensure accurate and complete source data when CPE data is used. This CVE-CPE mapping is used within the reporting component as an available option in custom reports.

Custom reporting features enable users to select all vulnerabilities in a given severity level, as well as define report parameters and options related to specific vulnerability categories and services, such as CPE, to display the CPE entries

corresponding to the displayed vulnerability, if any. SAINT's reporting options also enable users to select the output format from a number of available formats, such as HTML, XML and CSV.

CVE

CVE (Common Vulnerabilities and Exposures) is a dictionary of publicly known information security vulnerabilities and other information security exposures. The CVE repository is maintained by MITRE and is a free-use site. SAINT 8 provides support for CVE with the capability to execute vulnerability scans for vulnerabilities by CVE ID. SAINT 8 internally identifies vulnerabilities by its proprietary vulnerability check IDs and then cross-references with CVE names. SAINT 8 returns all vulnerability checks that detect the CVE and includes CVE numbers in its vulnerability data analysis, reports and tutorials for ease of reference to related tools and resources. At the conclusion of vulnerability scan execution, SAINT 8 provides users with the capability to view the list of vulnerabilities and continue the analysis by supporting customized scanning by selected CVE for a given vulnerability or by selecting other categories or values relevant to the analysis.

SAINT 8's analytical and report writing features then provide the capability to produce report output containing CVE IDs, in a number of formats, such as HTML, XML and CSV. SAINT 8 also provides hyperlinks to related resources, such as the SAINT on-line CVE Index, which includes the CVE ID, Description and custom SAINT tutorials; as well as linking directly to the official CVEs descriptions from the *Mitre.org CVE website* to facilitate further analysis, assessment and remediation.

CVE data is updated dynamically by SAINT as part of each release/update cycle – routinely twice each week. The "Generated Date" (by MITRE) and "Updated Date" (by SAINT) are part of this content. Note that there is a subclass of CVEs, called "candidates" that are potential CVEs but have not yet been approved. The candidate CVEs are prefixed by "CAN" in the SAINT/CVE cross-reference list. When candidates become approved in a new CVE version, they are moved from the "CAN" section of the cross-reference list to the "CVE" section, and then made available for report output and vulnerability tutorials. The SAINT/CVE cross-reference list includes CAN and CVE entries on the same page, so the browser's search function can search for both CVE and CAN entries when the YYYY-NNNN portion of the identifiers are specified in the search. The complete list of CVEs supported by SAINT can be found on our customer portal site *(mySAINT*).

CVSS

CVSS (Common Vulnerability Scoring System) is "a vulnerability scoring system designed to provide an open and standardized method for rating Information Technology vulnerabilities framework for communicating the characteristics and impacts of IT vulnerabilities". CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal, and environmental properties of a vulnerability. For more information see the *CVSS web site*.

SAINT 8 provides support for CVSS through scanning, analysis and reporting capabilities. SAINT 8 provides users with the capability to create custom scanning policies that include specified CVSS ranges when defining scan levels and setting up custom scans. SAINT 8's reporting options also enable the user to show the CVSS base score and CVSS base vector for each vulnerability detected, as an optional column, when creating custom reports. Custom reporting features within the Report tab enable users to select all vulnerabilities in a given severity level, as well as define report parameters and options related to specific vulnerability categories and services, such as CVSS base scores and CVSS base vectors, to display the CPE entries corresponding to displayed vulnerability, if any. SAINT 8 then enables users to select their output format from a number of available formats, such as HTML, XML and CSV. Additionally, SAINT 8 provides support for CVSS as part of Payment Card Industry (PCI) Compliance. CVSS base scores are shown in SAINT 8 as part of PCI compliance

reports. CVSS base scores are used as the primary factor in determining whether a given device is compliant during a PCI compliance assessment.

SAINT imports CVSS base scores, CVSS vectors and "date generated" from the *National Vulnerability Database (NVD)* and delivers that information, as well as the date updated by SAINT, to our customers through our SAINTexpress maintenance release process. The raw CVSS content is stored in the product database and is also available in the configuration sub-directory of the SAINT installation directory (e.g., config/cve-cvss). Each line in the cve-cvss file contains the name of the source file the data following that line was extracted from, along with both the "generated" and "updated" dates for the source file - prefixed with the "#" character.

Asset Identification (AI)

Asset Identification (AI), under SCAP, is a format for uniquely identifying assets based on known identifiers and/or known information about the assets. The SCAP specification describes the purpose of asset identification, a data model for identifying assets, methods for identifying assets, and guidance on how to use asset identification. It also identifies a number of known use cases for asset identification.

SAINT 8 supports the AI specification, version 1.1, by generating Asset Identifiers as part of the Asset Report Format (ARF) output. Output generated for scans are executed for any SCAP scan profile or benchmark, for both OVAL and XCCDF content. Asset identifiers are made available as content in the pre-configured ARF output in the SCAP module, by selecting a completed OVAL or XCCDF scan and viewing the ARF Report from the *Manage Results Data* page. Asset Identifiers are then available to users by selecting individual output files for any target assessed during the scan. The AI and ARF report can then be viewed within the SCAP user interface or exported in XML format to support local requirements and/or compliance reporting.

Asset Reporting Format (ARF)

The Asset Reporting Format (ARF), under SCAP, expresses the transport format of information about assets and the relationships between assets and reports. The SCAP specification prescribes the standardized data model to facilitate the reporting, correlating and fusing of asset information throughout and between organizations.

SAINT 8 supports the ARF specification, version 1.1, by generating ARF-formatted output. Output generated for scans are executed for any SCAP scan profile or benchmark, for both OVAL and XCCDF content. ARF formatted output is made available as pre-configured output in the SCAP module, by selecting a complete scan and viewing the SCAP-compatible results from the *Manage Results Data* page. The final ARF output is then made available as one of selectable output formats for individual targets assessed during the scan. The ARF report can then be viewed within the SCAP user interface or exported in XML format to support local requirements and/or compliance reporting.

Trust Model for Security Automation Data (TMSAD)

The SCAP Trust Model for Security Automation Data (TMSAD) is a specification for using digital signatures in a common trust model applied to other security automation specifications. The SCAP specification prescribes the standardized data model for establishing trust for security automation data.

SAINT 8 supports the TMSAD specification, version 1.0, by verifying the XML signature to ensure content has not been modified. If a signature is not valid, SAINT 8 aborts the scan and generates an error to notify the user of the failed scan.