Security Content Automation Protocol (SCAP)

SCAP Vendor Assertions Document v5.0

March 17, 2017

by

Rapid7 LLC

100 Summer Street, 13th Floor
Boston, MA 02110-2131

Tel: +1.617.247.1717

Fax: +1.617.507.6488

www.rapid7.com

For

Nexpose

Version 6.4.26**, CPE** cpe:/a:rapid7:nexpose:6.4.26

Assertion:

Rapid7 LLC asserts that Nexpose version 6.4.26 meets or exceeds the Derived Test Requirements (DTR) for SCAP Version 1.2 as described in NIST IR 7511 Revision 4.01 for the following SCAP capabilities and supported platform family:

Please copy "☑" into the column that contains "❑" for any supported Capabilities and 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

- ☑ Red Hat Enterprise Linux 5.11 Client 32 bit
- ☑ Red Hat Enterprise Linux 5.11 Client 64 bit

SCAP Component Technologies:

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

Please copy "☑" into "Supported" field for any supported Components.

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):

Statement of SCAP Implementation
Rapid7 Nexpose implements the Security Content Automation Protocol (SCAP) standard by implementing Common Vulnerability Enumeration (CVE), Common Platform Enumeration (CPE), and Common Vulnerability Scoring System (CVSS) standards. SCAP is a specification for expressing and manipulating security data in standardized ways.
In addition to supporting SCAP 1.2, Nexpose also supports backward compatibility with SCAP 1.0 and SCAP 1.1.
Nexpose implements the Common Vulnerability Enumeration (CVE) standard by assigning and displaying a CVE identifier for every vulnerability for which an identifier exists. Nexpose implements the Common Platform Enumeration (CPE) standard by assigning and displaying a CPE name for every asset for which a CPE name exists and mapping Nexpose fingerprints to their CPE counterparts.
Nexpose implements the Common Vulnerability Scoring System (CVSS) standard by computing the CVSS version 2 (CVSS v2) score index, which rates vulnerabilities according to the Forum of Incidence and Response Security Teams (FIRST) CVSSv2 specification for every discovered vulnerability.
Nexpose automatically includes SCAP content with each software update. For easier management, the Nexpose Security Console Web interface contains a dedicated SCAP Administration page, which indicates when SCAP content was most recently imported into Nexpose software. Four tables appear on the SCAP page:

- CPE Data
- CVE Data
- CVSS Data
- CCE Data

Each table lists a date for the most recent update as well as the generated date. The generated date indicates when the original CPE, CVE, and CVSS dictionaries were generated. CPE and CVE data is kept current through frequent data updates from the National Vulnerability Database. In addition, CVSS scores are maintained continuously through the MITRE-approved CVSS score algorithm built natively into Nexpose. Rapid7 is committed to continuous development of Nexpose in accordance with NIST SCAP guidelines.

Statement of CVE Implementation
Rapid7 Nexpose implements the Common Vulnerability Enumeration (CVE) standard by assigning and displaying a CVE identifier for every vulnerability for which an identifier exists. CVE is a format for describing information security vulnerabilities and exposures.
Every vulnerability Nexpose discovers in the scanning process appears in the vulnerability database. This extensive, full-text, searchable database also stores remediation information on patches and downloadable fixes, as well as reference content describing each security weakness. The database has been certified to be compatible with the MITRE Corporation's Common Vulnerabilities and Exposures (CVE) index. The MITRE Corporation standardizes the names of vulnerabilities across diverse security products and vendors. Users can search for vulnerabilities in the database through the Nexpose Security Console Web interface by using CVE identifiers as search criteria.
Each new Nexpose release uses the most current CVE listing. Every six hours, Nexpose updates its vulnerability definitions through a subscription service that both amends existing definitions and adds links for new CVE identifiers. In addition, Nexpose continually incorporates the most up-to-date CVE listing from the CVE mailing list and changelog. Multi-vector update capabilities ensure that Nexpose always performs vulnerability scanning with the newest CVE identifiers and descriptors .
The Web interface provides a centralized hub for viewing lists and comprehensive descriptions of all

instances of missing patches, software flaws, and vulnerabilities discovered on target systems, along with each any available corresponding CVE identifiers. The identifiers are hypertext links to external advisories on the National Institute of Standards (NIST) National Vulnerability Database, where additional relevant information may be found. CVE identifiers are displayed in the Discovered Vulnerabilities sections of Nexpose reports.

Statement of CPE Implementation

Rapid7 Nexpose implements the Common Platform Enumeration (CPE) standard by assigning and displaying a CPE name for every asset for which a CPE name exists. CPE is a structured naming scheme for hardware platforms, operating system platforms, and application platforms. The use of CPE names ensures that Nexpose consistently identifies scanned assets using industry-standard enumeration Nexpose scans operating systems, enterprise applications, databases, Web applications, and countless software packages on servers, workstations, networking devices, and other network-attached hardware. Built on a rules-based expert system, Nexpose can perform broader, deeper, and more accurate scans than any other vulnerability scanner on the market today. The adaptive scanning logic driven by the expert system recognizes target hardware platforms, operating system platforms, and application platforms. Nexpose's expert system applies all available CPE names to detected platforms.

Nexpose stores CPE names in its scan database and continually updates them by downloading changes from the centralized CPE dictionary maintained by the National Institute of Standards (NIST). Every revision to the CPE dictionary made by NIST is reflected in Nexpose, so Nexpose can map any new CPE names to application descriptions that previously did not have them.

Nexpose users have direct access to the CPE names in the following ways: Using the Nexpose Security Console Web interface they can view CPE names in scan data tables that list either all assets or just specific assets in a target environment, including software applications and operating systems. Also, Nexpose can generate Raw XML reports that contain CPE names. Users can then either view the CPE names in the raw XML format, or feed the XML data stream into other customized report formats.

Statement of CVSS Implementation

Rapid7 Nexpose implements the Common Vulnerability Scoring System (CVSS) standard by computing the CVSS version 2 (CVSS v2) score index for every discovered vulnerability. This index, which is managed by the Forum of Incidence and Response Security Teams (FIRST), provides an open framework for determining the relative severity of vulnerabilities and a standardized format for communicating vulnerability characteristics. A Nexpose algorithm computes each CVSS score based on severity level, ease of exploit, remote execution capability, credentialed access requirement, and other criteria. Nexpose displays CVSS scores in all vulnerability listings throughout the Nexpose Security Console Web interface. Each vulnerability is listed with its CVSS score and a corresponding Common Vulnerability Enumeration (CVE) identifier whenever a CVE identifier is available. Users factor in the CVSS score, severity rankings, and risk scores based on either temporal or weighted scoring models to prioritize vulnerability remediation tasks. Nexpose includes the CVSS score in all of its report templates. Allowing vulnerabilities to be quantified according to severity level and CVSS rating facilitates faster remediation. For example, reports that include the Highest Risk Vulnerability Details section list highest risk vulnerabilities and include their categories, risk scores, and their CVSS scores. Reports that include the Index of Vulnerabilities section include the severity level and CVSS rating for each vulnerability.

The CVSS score is the primary factor in determining whether a given device is compliant with Payment Card Industry (PCI) standards. Nexpose incorporates CVSS scores in its PCI Audit Report, which provides detailed PCI compliance audit results. The PCI Vulnerability Details section of the PCI Audit Report contains in-depth information about each vulnerability discovered during the PCI Audit scan. Each discovered vulnerability is ranked according to its CVSS score. Nexpose is a Payment Card Industry (PCI)-

sanctioned tool for conducting compliance audits, and Rapid7 is an Approved Scanning Vendor (ASV). Rapid7 customers can further leverage their Nexpose investments with ongoing scans to track their CVSS scores in preparation for quarterly PCI audits. This comprehensive CVSS coverage provides companies with strong decision support, which cuts response times for detected vulnerabilities.
In addition to the actual CVSS score, Nexpose enables users to configure their own customized risk scoring based on the specific needs of their unique environment. Customized risk scoring, together with the standardized CVSS score, provides a unique opportunity for security administrators to manage their risk exposure with the most granularity and precision available in our industry.

Statement of CCE Implementation
Rapid7 Nexpose implements the Common Configuration Enumeration (CCE) standard by associating an appropriate CCE identifier with the relevant test result configuration statement. The CCE identifiers are derived from Security Content Automation Protocol (SCAP) content imported by Rapid7 Nexpose, and reflect the latest version of the Common Configuration Enumeration List.
When used as a Federal Desktop Core Configuration (FDCC) scanner, Rapid7 Nexpose produces an eXtensible Configuration Checklist Description Format (XCCDF)-compliant report. In compliance with the XCCDF results format, each test result contains a field that lists the CCE identifier that is relevant to the test result. The CCE identifiers can be extracted from the report using regular expressions or XML parsing tools. Rapid7 Nexpose can also produce the result report file in additional formats, including plain text, and users have the option to create their own tools for converting XCCDF-compliant reports into their preferred format. Regardless of the result report format, the field containing the CCE identifier associated with a given test result is listed.

Statement of XCCDF Implementation
Rapid7 Nexpose implements the eXtensible Configuration Checklist Description Format (XCCDF) by providing the ability to import Security Content Automation Protocol (SCAP) content that includes XML files in XCCDF-compliant format. Rapid7 Nexpose implements validation routines that ensure that imported XCCDF content is compliant with the standard by checking the files against schema documents. If any of the XCCDF content is invalid according to the XCCDF schema, Rapid7 Nexpose reports an error in the import process.
Rapid7 Nexpose evaluates valid Open Vulnerability Assessment Language (OVAL) definition files against a specified target system in conjunction with the associated XCCDF content and produces a result report in valid XCCDF format. Rapid7 Nexpose ensures that the XCCDF result reports are valid XCCDF. Rapid7 Nexpose can also produce the result report file in additional formats, including plain text, and users have the option to create their own tools for converting XCCDF-compliant reports into their preferred format.

Statement of OVAL Implementation
Rapid7 Nexpose implements the eXtensible Open Vulnerability Assessment Language (OVAL) by providing the ability to import Security Content Automation Protocol (SCAP) content that includes XML files in OVAL-compliant format. Rapid7 Nexpose implements validation routines that ensure that imported OVAL content is compliant with the standard by checking the files against schema documents. If any of the OVAL content is invalid according to the OVAL schema, Rapid7 Nexpose reports an error in the import process.
Rapid7 Nexpose evaluates valid OVAL definition files against a specified target system in conjunction with the associated eXtensible Configuration Checklist Description Format (XCCDF) content and produces result files for each definition using the OVAL full results format, along with a result report in valid XCCDF format. Rapid7 Nexpose can also produce the result report file in additional formats, including plain text, and users have the option to create their own tools for converting XCCDF-compliant

reports into their preferred format.

SCAP Backwards Compatibility:

In addition to supporting SCAP 1.2 and the ability to upload datastreams and datastream collection formats, Nexpose also supports backward compatibility with SCAP 1.0 and SCAP 1.1 formats. Users are able to upload ZIP or JAR archives in the earlier formats, using the Upload Policy feature on the Policies page of the Nexpose Security Console Web interface. The Security Console continues to display explicit messages to address any formatting errors related to these archives, and all of these messages are explained in detail in the Nexpose online Help (available with the product) and user's guide (available in the Rapid7 online community. After uploading the archives, users can incorporate Extensible Configuration Checklist Description Format (XCCDF) profiles into scans, either by selecting specific built-in scan templates or creating custom scan templates and selecting certain policies and benchmarks. Because Nexpose continues to support the earlier formats of the XCCDF reporting schema, users can generate XML export or human-readable reports with XCCDF-formatted policy and benchmark scan results. If an SCAP 1.1 datastream is uploaded, the report will be output in an SCAP 1.2-compliant format.

Disclaimer:

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