BMC Client Management - SCAP Implementation Statement

Version 12.0

BUSINESS RUNS ON I.T.
I.T. RUNS ON BMC™

www.bmc.com

Contents

SCAP Implementation Statement

The SCAP features in BMC Client Management comply with the Technical Specification for the Security Content Automation Protocol (SCAP): Version 1.2. Using features in the BMC Client Management Console, you import SCAP content from third-party sources, such as the NIST NVD National Checklist Program repository. Results are generated as XML files compliant with both the SCAP (for ARF) and XCCDF specifications.

BMC Software, Inc. asserts that BMC Client Management (BCM) version 12.00.00 meets or exceeds the Derived Test Requirements (DTR) for SCAP 1.0, 1.1 and 1.2 as described in NIST IR 7511 Revision 3 for the following SCAP capabilities and supported platform family:

Capabilities

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

Platform Families

- Microsoft Windows 7, 64 bit
- Microsoft Windows 7, 32 bit
- Microsoft Windows Vista, SP2
- Microsoft Windows XP Pro, SP3
- Red Hat Enterprise Linux 5 Desktop, 64 bit
- Red Hat Enterprise Linux 5 Desktop, 32 bit

BMC Client Management additionally provides SCAP capabilities for systems such as MAC OS X and other Windows/Linux flavors, but these are not certified.

SCAP 1.2 Conformance

BMC Client Management conforms to the specifications of the Security Content Automation Protocol, version 1.2 (SCAP 1.2), as outlined in NIST Special Publication (SP) 800-126 rev 2. As part of the SCAP 1.2 protocol, BMC Client Management assessment capabilities have been expanded to include the consumption of source data stream collection XML files and the generation of well-formed SCAP result data streams.

To exercise this capability, users may download the SCAP 1.2 content from the NIST NVD National Checklist Program repository, or any other source of SCAP 1.2 compliant content, and perform assessments in a similar manner as with BMC Client Management custom compliance.

The BMC Client Management implementation includes the following components:

- Extensible Configuration Checklist Description Format (XCCDF) 1.2, a language for authoring security checklists/benchmarks and for reporting results of evaluating them.
- Open Vulnerability and Assessment Language (OVAL) 5.10.1, a language for representing system configuration information, assessing machine state, and reporting assessment results.
- Asset Reporting Format (ARF) 1.1, a format for expressing the transport format of information about assets and the relationships between assets and reports.
- Asset Identification 1.1, a format for uniquely identifying assets based on known identifiers and/or known information about the assets.
- Common Platform Enumeration (CPE) 2.3, a nomenclature and dictionary of hardware, operating systems, and applications.
- Common Configuration Enumeration (CCE) 5, a nomenclature and dictionary of software security configurations.
- Common Vulnerabilities and Exposures (CVE), a nomenclature and dictionary of security-related software flaws.
- Common Vulnerability Scoring System (CVSS) 2.0, a system for measuring the relative severity of software flaw vulnerabilities.

- Common Configuration Scoring System (CCSS) 1.0, a system for measuring the relative severity of system security configuration issues. BMC Client Management supports CCSS scores when that score is used in the @weight attribute within XCCDF rules.
- Trust Model for Security Automation Data (TMSAD) 1.0, a specification for using digital signatures in a common trust model applied to other security automation specifications. BMC Client Management can import SCAP content with Trust Model for Security Automation Data (TMSAD) signatures but will not verify them. The generated XML report will not include TMSAD signatures.

SCAP 1.0 Compatibility

BMC Client Management natively supports the older SCAP 1.0 specification, including:

- Extensible Configuration Checklist Description Format (XCCDF) version 1.1.4
- Open Vulnerability and Assessment Language (OVAL), version 5.3 and 5.4
- Common Configuration Enumeration (CCE) version 5
- Common Platform Enumeration (CPE) version 2.2
- The Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS) version 2.0

SCAP 1.1 Compatibility

BMC Client Management natively supports the older SCAP 1.1 specification, including:

- Extensible Configuration Checklist Description Format (XCCDF) version 1.1.4
- Open Vulnerability and Assessment Language (OVAL) version 5.8
- Common Configuration Enumeration (CCE) version 5
- Common Platform Enumeration (CPE) version 2.2
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS) version 2.0

CVE and CCE lists

BMC Client Management allows to import CVE and CCE lists. Both of these lists are part of the six existing open standards used by NIST in its Security Content Automation Protocol (SCAP) program. They help, through the use of consistent identifiers, to improve data correlation; enable interoperability; foster automation; and ease the gathering of metrics for use in situation awareness, IT security audits, and regulatory compliance. CVE provides this capability for information security vulnerabilities, CCE assigns a unique, common identifier to a particular security-related configuration issue:

- CVE ® (Common Vulnerabilities and Exposures) is a dictionary of common names (that is, CVE Identifiers) for publicly known information security vulnerabilities. CVE is now the industry standard for vulnerability and exposure names. CVE Identifiers provide reference points for data exchange so that information security products and services can speak with each other.
- CCE (Common configuration Enumeration) lists provide unique identifiers to security-related system configuration issues in order to improve workflow by facilitating fast and accurate correlation of configuration data across multiple information sources and tools.