SCAP 1.2 Overview

Karen Scarfone

Scarfone Cybersecurity

Agenda

- **Introduction to SCAP**
- What's Changed from SCAP 1.1 to 1.2
  - SCAP 1.2 Conformance (800-126 Section 2)
  - SCAP Content Requirements and Recommendations (Section 3)
  - SCAP Content Processing Requirements and Recommendations (Section 4)
  - Source Data Stream Content Requirements for Use Cases (Section 5)

The Need for Security Automation: Tools and Content

- Security tools
  - Vulnerability, configuration, and patch scanners and management tools
  - Intrusion detection/prevention systems
  - Antivirus software, other antimalware tools
  - Many others
- Security content
  - Knowledge about vulnerabilities and threats
  - Security checklists
  - Requirements from mandates, etc.
- Proprietary methods for data sharing, analysis, aggregation, etc.
  - Significant time and resources to achieve interoperability
  - Ambiguity in translation and understanding
  - Massive duplication of effort

The Need for Security Automation: Challenges

- Many operating systems and applications to secure and monitor
  - High number of configuration settings, patches, etc.
  - Time and resource intensive + boring = lots of opportunities for mistakes
- Address new vulnerabilities and threats quickly
- Culture shift from occasional audits to continuous monitoring and dashboards
- Many requirements to meet and provide evidence of compliance with
  - Standards, frameworks, regulations, guidelines
- Lack of interoperability between products

What Is SCAP?

- A standardized approach to maintaining the security of enterprise systems
- Comprised of
  - A set of individually maintained, community developed open specifications that…
    - Standardize the security information we communicate—**content**
    - Standardize how we communicate and use security information—**tools/content processing**
  - Additional specifications that define how these individual specifications interact with each other
  - Standardized reference data (e.g., NVD)

SCAP 1.2 Specifications

Languages: Means of providing instructions and reporting results	eXtensible Checklist Configuration Description Format (XCCDF) 1.2
	Open Vulnerability and Assessment Language (OVAL) 5.10
	Open Checklist Interactive Language (OCIL) 2.0
Reporting formats: Express collected info in standard formats	Asset Reporting Format (ARF) 1.1
	Asset Identification 1.1
Enumerations: Conventions for identifying and naming	Common Vulnerabilities and Exposures (CVE)
	Common Configuration Enumeration (CCE) 5
	Common Platform Enumeration (CPE) 2.3
Measurement and scoring systems: Risk measurement	Common Vulnerability Scoring System (CVSS) 2.0
	Common Configuration Scoring System (CCSS) 1.0
Integrity: Preserve integrity of SCAP content and results	Trust Model for Security Automation Data (TMSAD) 1.0

Interoperability Example

XCCDF Checklist (Instructions)

- CPE names for the applicable platforms
- Calls to OVAL definitions
- Calls to OCIL questionnaires
- Checklist signed by TMSAD

OVAL Definitions (Test Procedures)

- CCE names for configuration definitions
- CVE names for vulnerability and patch definitions
- CPE names for inventory definitions

Enumerations

- CCE lists
- CVE dictionary
- CPE list

Results

- ARF report format
  - Uses Asset Identification
- Report signed by TMSAD

Measurement and Scoring Systems

- CVSS metrics for CVE names
- CCSS metrics for CCE names

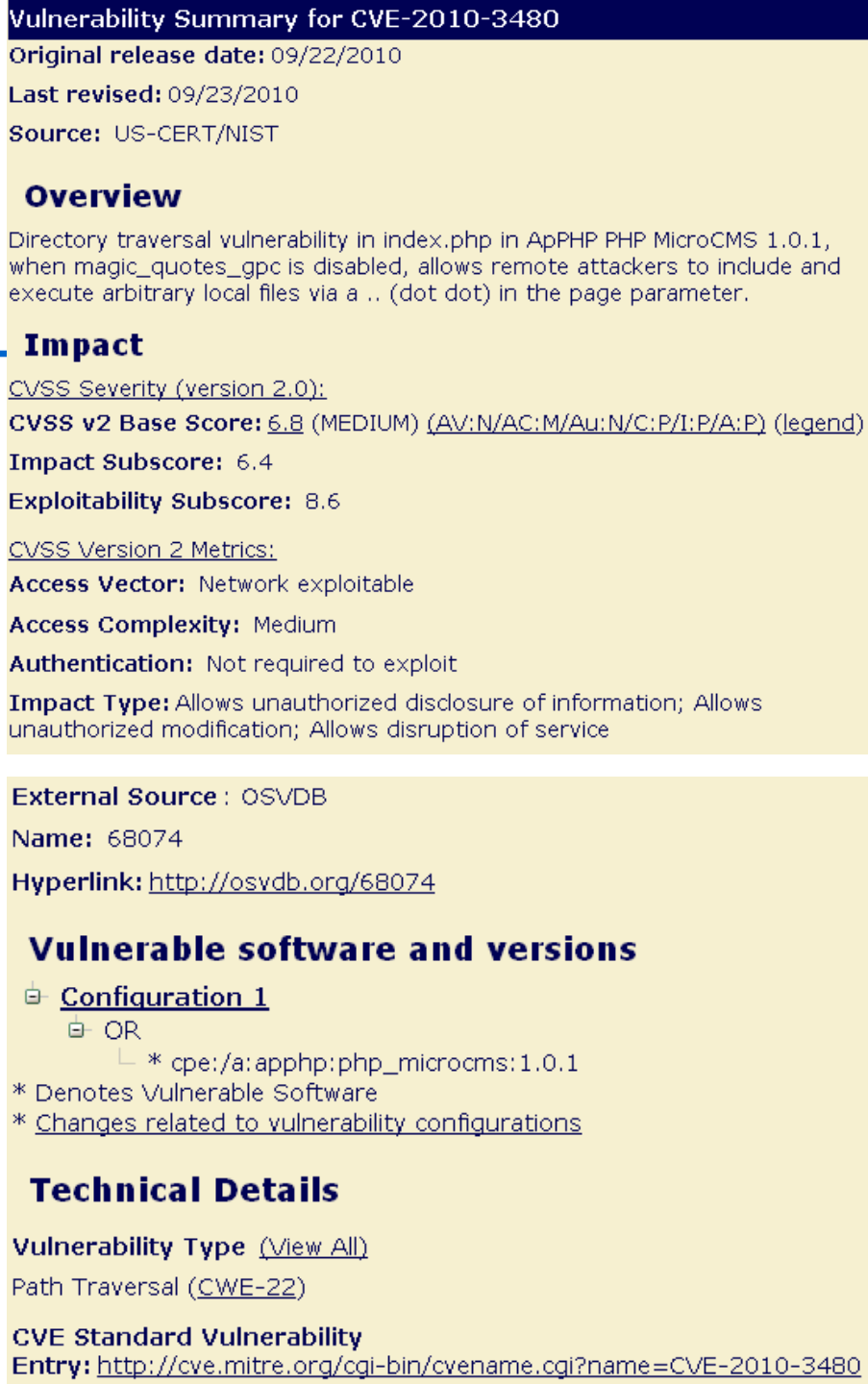
Examples of Common SCAP Uses

- Security configuration verification
  - Compare settings in a checklist to a system's actual configuration
  - Verify configuration before deployment, audit/assess/monitor operational systems
  - Map individual settings to high-level requirements (requirements traceability)
  - Similar process for verifying patch installation and identifying missing patches
- Check systems for signs of compromise
  - Known characteristics of attacks, such as altered files or the presence of a malicious service

Existing SCAP Content

National Vulnerability Database (NVD)

- http://nvd.nist.gov/download.cfm
- Data on over 48,000 CVE identifiers, including CVSS metrics and scores
- CPE product dictionary
- Search engines, XML feeds, and RSS feeds available



Vulnerability Summary for CVE-2010-3480

Original release date: 09/22/2010

Last revised: 09/23/2010

Source: US-CERT/NIST

Overview

Directory traversal vulnerability in index.php in ApPHP PHP MicroCMS 1.0.1, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the page parameter.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 6.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:P) (legend)

Impact Subscore: 6.4

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

External Source : OSVDB

Name: 68074

Hyperlink: http://osvdb.org/68074

Vulnerable software and versions

Configuration 1

OR

* cpe:/a:apphp:php_microcms:1.0.1

* Denotes Vulnerable Software

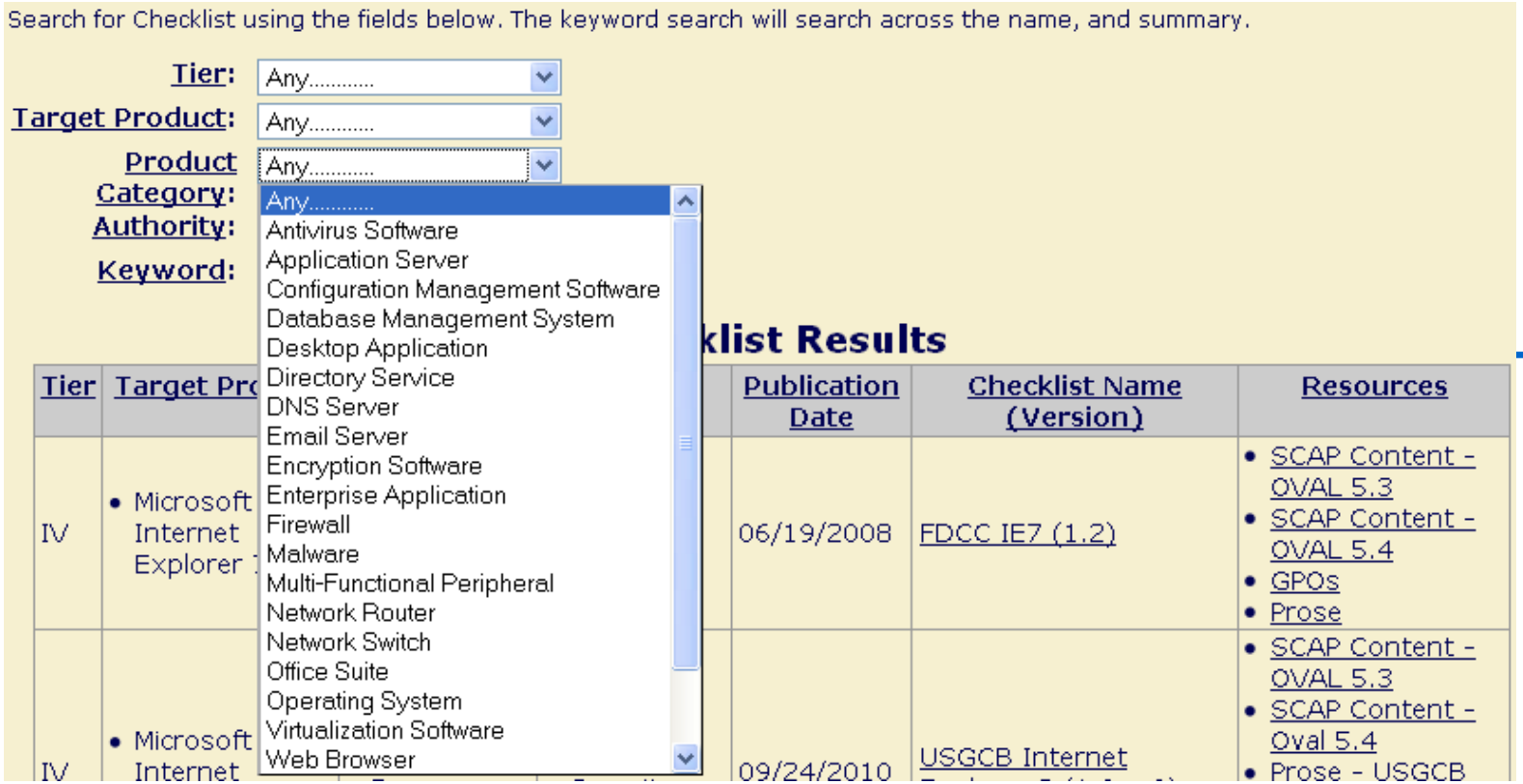
* Changes related to vulnerability configurations

Technical Details

Vulnerability Type (View All)

Path Traversal (CWE-22)

CVE Standard Vulnerability Entry: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3480



- National Checklist Program (NCP) Repository
  - http://web.nvd.nist.gov/view/ncp/repository
  - Repository of publicly available security configuration checklists
  - Over 150 checklists: combination of SCAP, proprietary, and prose formats

SCAP Documentation

- NIST Special Publication (SP) 800-117, Guide to Adopting and Using SCAP
  - Provides an overview of SCAP
  - Focuses on how organizations can use SCAP-enabled tools to enhance their security posture
  - Explains to product and service vendors how they can adopt SCAP within their offerings
- NIST SP 800-126 Revision 2, The Technical Specification for SCAP
  - Definitive technical specification for SCAP v 1.2
  - Describes the basics of the SCAP component specifications and their interrelationships, the characteristics of SCAP content, and all SCAP requirements not already defined elsewhere
- NIST SP 800-70 Revision 2, National Checklist Program for IT Products
  - Explains how to use the NIST National Checklist Program (NCP) to find and retrieve checklists
  - Describes the policies, procedures, and other requirements for participation in the NCP

Additional SCAP Documentation

http://scap.nist.gov/index.html

http://scap.nist.gov/revision/1.2/index.html

- Pointers to documentation and other information for individual specifications
- SCAP Content Validation Tool

http://scap.nist.gov/validation/index.html

- Information on the SCAP Validation Program

Component Specification Changes (Section 2 intro)

- Added specs
  - Asset Reporting Format (ARF) 1.1
  - Asset Identification 1.1
  - Common Configuration Scoring System (CCSS) 1.0
  - Trust Model for Security Automation Data (TMSAD) 1.0
- Updated specs
  - XCCDF from 1.1.4 to 1.2
  - OVAL from 5.8 to 5.10
  - CPE from 2.2 to 2.3
- Unchanged specs
  - OCIL, CCE, CVE, CVSS
- Will publish errata for SP 800-126
  - Errata overrides requirements in SP 800-126 and component specifications

Agenda

- Introduction to SCAP
- **What's Changed from SCAP 1.1 to 1.2**
  - **SCAP 1.2 Conformance (800-126 Section 2)**
  - SCAP Content Requirements and Recommendations (Section 3)
  - SCAP Content Processing Requirements and Recommendations (Section 4)
  - Source Data Stream Content Requirements for Use Cases (Section 5)

SCAP-conformant products (2.1)

- **Content producer:** a product that generates SCAP source data stream content
- **Content consumer:** a product that accepts existing SCAP source data stream content, processes it, and produces SCAP result data streams
- Many requirements are now tagged as applying to only one product type (content producer, content consumer)
  - Was implied before but never stated explicitly

Source Content Conformance (2.2)

- Section used to give requirements for “organization conformance”
- Terminology has changed from “organization” to “source content”
- Requirements essentially the same with one key difference: now specific to source data streams only
  - Previously talked about “SCAP content”, which could be interpreted to include result content

Agenda

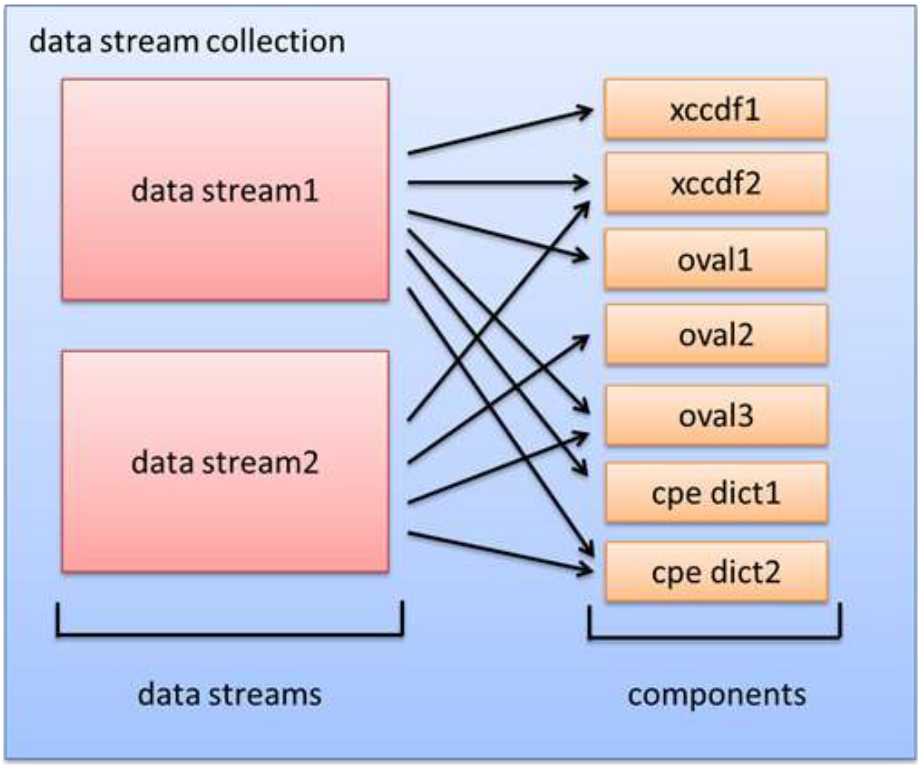
- Introduction to SCAP
- What's Changed from SCAP 1.1 to 1.2
  - SCAP 1.2 Conformance (800-126 Section 2)
  - **SCAP Content Requirements and Recommendations (Section 3)**
  - SCAP Content Processing Requirements and Recommendations (Section 4)
  - Source Data Stream Content Requirements for Use Cases (Section 5)

SCAP Content Requirements and Recommendations (Section 3)

- SCAP Source Data Stream (3.1)
- XCCDF (3.2)
- OVAL (3.3)
- OCIL (3.4)
- CPE (3.5)
- CCE, CVE, CVSS, CCSS (3.6-3.9)
- XML Digital Signatures (3.10)

SCAP Source Data Stream (3.1)

- Greatly revised and expanded section
- Collection of links to source components, such as XCCDF checklists, OVAL documents, and CPE dictionaries
- Multiple instances of one source component type permitted
- Links may be in any order
- Defined in data model and XML schema



Source Data Stream Validation (3.1.2)

- Supports tailoring (<xccdf:Tailoring> element)
- All referenced components SHALL validate against the corresponding component schema and its embedded Schematron rules
- If applicable, each component MUST validate against its associated Schematron stylesheet
  - Authoritative Schematron stylesheets will be maintained on the SCAP website (http://scap.nist.gov/revision/1.2/#schematron)
  - SCAP errata document will note all changes

Data Stream Globally Unique Identifiers (3.1.3)

- Mandatory conventions for certain identifiers
  - *namespace* is a reverse-DNS style string associated with the content author
  - *name* is an NCName-compliant string

Element	Identifier Format Convention
<ds:data-stream-collection>	scap_*namespace*_collection_*name*
<ds:data-stream>	scap_*namespace*_datastream_*name*
<ds:component-ref>	scap_*namespace*_cref_*name*
<ds:component>	scap_*namespace*_comp_*name*
<ds:extended-component>	scap_*namespace*_ecomp_*name*

1:15 tomorrow: Adam Halbardier,
SCAP 1.2 Datastream Formats

XCCDF: Update from 1.1.4 to 1.2

- NISTIR 7275r4 has been completely reorganized from the previous revision
  - Detailed change log in Appendix B includes mappings from old sections to new sections, and lists of functional and editorial changes
  - New conformance section
  - RFC 2119 (SHALL, SHOULD, MAY) language being used throughout
  - Glossary added

XCCDF: Update from 1.1.4 to 1.2 (cont.)

- XCCDF namespace changed; version 1.2 not backwards compatible with version 1.1.4
- CPE 2.3 required for platform specification
  - Formatted string bindings recommended, URI bindings permitted
- Mandatory standard format for the identifiers of major elements (to enable global uniqueness)
- Metadata fields added to all major elements
- New top-level Tailoring element; new concept of a tailoring document

3:45 today: Charles Schmidt, XCCDF 1.2 Update

XCCDF (3.2)

- Reorganization of the section
- Prohibits:
  - XInclude elements in XCCDF content
  - <xccdf:set-complex-value> elements within <xccdf:Profile> elements
  - <xccdf:source>, <xccdf:complex-value>, or <xccdf:complex-default> elements within <xccdf:Value> elements
  - use of XCCDF group extension
- CCSS support added; use completely optional (MAY)

XCCDF (cont.)

- Clarified unique identification of benchmark revisions
  - <xccdf:version> and @id attribute used together
- Clarified use of <xccdf:ident>, <xccdf:check-content-ref> elements

OVAL: Update from 5.8 to 5.10

Updates in OVAL 5.9:

- “A significant refactoring of the XML Schema definition of the record datatype in the oval-system-characteristics-schema and the oval-definitions-schema to address an invalid XML Schema construct that was reported by the community.
- Removes an improper use of the xpath 2.0 exists() function
- Corrects the mac-os:pwpolicy_object
- Adds a Schematron rule to ensure proper use of the filename entity.”

Source: http://oval.mitre.org/news/index.html#feb222011a

2:30 today: Jon Baker, OVAL 5.10 Update

OVAL: Update from 5.8 to 5.10 (cont.)

Updates in OVAL 5.10:

- “New test to support using PowerShell cmdlets to collect system state information (win-def:cmdlet_test)
- New win-def:peheader_test
- Corrected Schematron rules for objects in EntityAttributeGroup that did not account for the new EntityObjectRecordType
- Added documentation on implementing the operations for the fileset_revision datatype
- Added instance entity to the macos-def:plist_object -and creation of macos-def:plist510_object
- Addition of last_logon entity to win-def:user_state, win-sc:user_item, unix-def:password_state, and unix-sc:password_item”

Source: http://oval.mitre.org/news/index.html#sep142011a

OVAL: Update from 5.8 to 5.10 (cont.)

Updates in OVAL 5.10 (cont.):

- “Clarified documentation around handling of recording partial matches in system characteristics items
- Clarified documentation and added dependency_check_passed, digest_check_passed, verification_script_successful, and signature_check_passed entities to the lin-def:rpmverify_test
- Corrected conflicting and invalid documentation of the mask attribute
- Added win-def:sharedresourceeffectiverights_test and win-def:sharedresourceauditedpermissions_test
- Corrected several issues in the sharepoint component schema.”

Source: http://oval.mitre.org/news/index.html#sep142011a

OVAL (3.3)

- Default OVAL version bumped from 5.8 to 5.10; minimum supported is still 5.3
- Specifies required values for @class attribute
  - Making sure each definition class is used as intended
- May mix types of definitions within a single OVAL component
- May have multiple OVAL components with definitions grouped by “least version”

OCIL (3.4)

- Added <ocil:reference> element recommendations
  - Map OCIL questionnaires to associated CCE, CVE, and/or CPE identifiers

CPE (update from 2.2 to 2.3)

- Split into four modular specifications (IRs 7695-7698)
- Introduces the well-formed name (WFN) concept
- New CPE name formats
  - *Formatted string binding*
    cpe:2.3:a:microsoft:internet_explorer:8.0.6001:beta:*:*:*:*:*:*
  - *URI binding*
    cpe:/a:microsoft:internet_explorer:8.0.6001:beta
- URI binding provides backwards compatibility with CPE version 2.2

CPE (cont.)

- Name Matching specification
  - Eliminated the prefix property from CPE 2.2
  - Redefines name matching set relations (SUPERSET, SUBSET, EQUAL, DISJOINT)
    - Explains how to implement CPE 2.2 equivalent matching capabilities using CPE 2.3
  - Defines name matching in terms of WFNs so as to be agnostic in regards to name bindings
  - Attribute comparisons include single-character and multi-character wild cards

CPE (cont.)

- Dictionary specification
  - Updated deprecation logic; now includes one-to-many CPE deprecation
  - Updates to change history and provenance data requirements
  - Built-in one-to-one mapping between CPE 2.2 and CPE 2.3 names
    - CPE 2.3 name is embedded into the element holding the CPE 2.2 name

CPE (cont.)

- Applicability Language specification
  - Name changed from “Language” to “Applicability Language”
  - Updated namePattern type
    - Supports both formatted string and URI bindings

1:30 today: Chris McCormick,
NVD CPE Dictionary Management Practices

CPE (3.5)

- Subset of the official dictionary may be used
- Third party dictionaries and subsets of third party dictionaries may be used
- Dictionary components may be remote or local
- Each CPE name in <xccdf:platform> or <cpe2:fact-ref> elements within XCCDF documents MUST match at least one entry in one of the designated dictionary components

CCE, CVE, CVSS, CCSS (3.6-3.9)

- CCE, CVE, and CVSS requirements unchanged
- New Section 3.9 on CCSS
  - Similar to CVSS, but used for security configuration settings instead of software flaw vulnerabilities
  - CCSS may be supported by products
  - No requirements specific to CCSS use (only MAY statements)
  - At this time, no CCSS data repositories are publicly available

10:30 tomorrow: Karen Scarfone, CCSS

XML Digital Signatures (3.10)

- New TMSAD 1.0 specification
  - Makes extensive use of W3C recommendation *XML Signature Syntax and Processing* (also known as XMLDSIG)
  - Defines a small data model and schema
  - Specifies which signature and hash algorithms must be supported (and required parameters)
  - Places additional requirements on XMLDSIG

4:45 today: Harold Booth, A Trust Model for Security Automation Data

XML Digital Signatures (3.10 cont.)

- Several additional requirements in SP 800-126 above what TMSAD requires
  - Makes some elements mandatory
  - Specifies some element sequences
  - Defines how other elements (components, data streams, etc.) must be referenced by the digital signature elements

Agenda

- Introduction to SCAP
- What's Changed from SCAP 1.1 to 1.2
  - SCAP 1.2 Conformance (800-126 Section 2)
  - SCAP Content Requirements and Recommendations (Section 3)
  - **SCAP Content Processing Requirements and Recommendations (Section 4)**
  - Source Data Stream Content Requirements for Use Cases (Section 5)

SCAP Content Processing Requirements and Recommendations (Section 4)

- Legacy Support (4.1)
- Source Data Streams (4.2)
- XCCDF Processing (4.3)
- Result Data Streams (4.4)
- XCCDF Results (4.5)
- OVAL Results (4.6)
- OCIL Results (4.7)
- Result Data Stream Signing (4.8)

Legacy Support (4.1)

- Content consumers SHALL process SCAP 1.2 content and SCAP 1.0 content
  - As defined under the corresponding SP 800-126 version
- Content consumers that process legacy SCAP content
  - MUST be capable of outputting results in the same SCAP version as the source content
  - MAY convert the legacy SCAP results into SCAP 1.2 results
- Content consumers MUST support all deprecated constructs because they are still valid
- Content consumers supporting OVAL SHALL support OVAL Definition documents written against OVAL 5.3-5.10

Source Data Streams (4.2)

- Content consumers SHALL be capable of:
  - Validating SCAP content against the appropriate schemas and Schematron stylesheets
    http://scap.nist.gov/revision/1.2/#schema
    http://scap.nist.gov/revision/1.2/#schematron
  - Detecting and reporting errors, and failing gracefully if there are errors
- Content consumers SHOULD validate XML digital signatures in the source content
- Unrecognized <ds:extended-component> elements SHALL cause a warning
- Requirements for indicating which data stream and benchmark to evaluate

XCCDF Processing (4.3)

- Added significantly more detail on how CPE applicability processing must be performed
- Clarified the process for resolving <xccdf:check-content-ref> elements
- Added requirements related to unsupported check systems (unsupported by SCAP, unsupported by processing tool)

SCAP Result Data Streams (4.4)

- Greatly revised and expanded section
- Similar in concept to source data streams
- Uses the Asset Reporting Format (ARF) specification
  - Requirements and recommendations for using ARF for XCCDF, OVAL, and OCIL component reporting
  - No longer any filename suffix requirements
  - Target asset identification requirements
  - ARF relationship requirements

11:30 tomorrow: Adam Halbardier,
ARF 1.1 and Asset Identification 1.1

XCCDF Results (4.5)

- Deleted several existing requirements that are included in XCCDF 1.2
- Clarified processing of <xccdf:ident> elements
- Added the @con:negate attribute
- Required <xccdf:target-id-ref> with particular attribute values
- Clarified <xccdf:rule-result> requirements, including generalizing it to include CVE, CCE, and CPE (CPE not previously included)
- Reduced # of <xccdf:fact> elements to report

OVAL Results (4.6)

- OVAL result data stream components SHALL validate against the 5.10 results schema
- Clarified <oval-res:ContentEnumeration> element use in the data results
- Defined reference conventions for specifying OVAL system characteristics

OCIL Results (4.7)

- Unchanged

Result Data Stream Signing (4.8)

- New section
- Uses the new TMSAD 1.0 specification
- Several additional requirements in SP 800-126 above what TMSAD requires (similar in nature to source data stream signing reqs)
  - Makes some elements mandatory
  - Specifies some element sequences
  - Defines how other elements (components, data streams, etc.) must be referenced by the digital signature elements

4:45 today: Harold Booth, A Trust Model for Security Automation Data

Agenda

- Introduction to SCAP
- What's Changed from SCAP 1.1 to 1.2
  - SCAP 1.2 Conformance (800-126 Section 2)
  - SCAP Content Requirements and Recommendations (Section 3)
  - SCAP Content Processing Requirements and Recommendations (Section 4)
  - **Source Data Stream Content Requirements for Use Cases (Section 5)**

Source Data Stream Content Requirement for Use Cases (5)

- Compliance Checking
- Vulnerability Scanning
- Inventory Scanning
  - Includes malware artifact detection
- OVAL-Only Scanning use case has been dropped
- Requirements for which OVAL definitions, etc. go into each component have been changed because of the new source data stream model

References (new/changed only)

- SP 800-126 Revision 2 (SCAP 1.2)
  http://csrc.nist.gov/publications/PubsSPs.html#800-126
- IRs 7693-7694 (ARF 1.1 and Asset Identification 1.1)
  http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7694
- IR 7502 (CCSS 1.0)
  http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7502
- IRs 7695-7698 (CPE 2.3)
  http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7695
  http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7696
  http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7697
  http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7698
- OVAL 5.10
  http://oval.mitre.org/language/version5.10/
- IR 7802 (TMSAD 1.0)
  http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7802
- IR 7275 Revision 4 (XCCDF 1.2)
  http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7275

Questions & Answers / Feedback

Karen Scarfone

Scarfone Cybersecurity

karen@scarfonecybersecurity.com

(703) 401-1018