# SCAP Overview


Karen Scarfone
September 27, 2010

# SCAP 101 Tutorial Track

- High-level overview of SCAP and each of the component specifications it references
- Agenda
  - 10:45 – 11:30: SCAP Overview, Karen Scarfone, G2
  - 11:45 – 12:30: XCCDF Tutorial, Bryan Worrell, MITRE
  - 12:30 – 1:30: Lunch, Vendor Expo Hall
  - 1:30 – 2:15: OVAL Tutorial, Matt Hansbury, MITRE
  - 2:30 – 3:15: Standards Toolkit, Dave Mann, MITRE
  - 3:15 – 3:45: Break, Vendor Expo Hall
  - 3:45 – 4:30: CCE and CPE Tutorials, Dave Mann, MITRE
  - 4:45 – 5:30: CVE and CVSS, Steve Christey, MITRE
  - 5:30 – 7:00: Reception, Vendor Expo Hall and Foyer

# SCAP Overview Agenda

- The Need for Security Automation
- Introduction to SCAP
- Uses for SCAP
- SCAP Adoption
- SCAP Validation Program
- SCAP Lifecycle

Substantially based on NIST SP 800-117, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0,* and NIST SP 800-126, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0*
http://csrc.nist.gov/publications/PubsSPs.html

# 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
  - Several thousand new software flaws announced annually
- 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 1.0 Specifications

| | | | |
|---|---|---|---|
| **Languages: Means of providing instructions and reporting results** | **eXtensible Checklist Configuration Description Format (XCCDF) 1.1.4** | NSA and NIST | XML-based language for specifying checklists and reporting the results of checklist evaluation |
| | **Open Vulnerability and Assessment Language (OVAL) 5.3 and 5.4** | MITRE | XML-based language for specifying test procedures to detect machine state |
| **Enumerations: Conventions for identifying and naming** | **Common Vulnerabilities and Exposures (CVE)** | MITRE | Nomenclature and dictionary of security-related software flaws |
| | **Common Configuration Enumeration (CCE) 5** | MITRE | Nomenclature and dictionary of software security configuration issues |
| | **Common Platform Enumeration (CPE) 2.2** | MITRE | Nomenclature and dictionary for product names and versions |
| **Metrics: Risk measurement** | **Common Vulnerability Scoring System (CVSS) 2.0** | FIRST | Methodology for measuring the relative severity of software flaw vulnerabilities |

# Specification Interoperability Example

XCCDF Checklist (Instructions)

- CPE names for the applicable platforms
- Calls to OVAL definitions

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

Metrics

- CVSS metrics for CVE names

# Common Uses of SCAP

- 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

# Common Uses of Individual SCAP Specifications

- Standardized security enumerations (CVE, CCE, CPE)
  - Interoperability for security management tools, such as vulnerability scanners and patch management utilities
  - Information sharing, such as security bulletins and incident reports
- Vulnerability remediation prioritization (CVSS)
  - Use scores of relative vulnerability severity to help prioritize remediation, such as applying patches

# Adopting SCAP: Roles

- Software Developers
  - Register and use standardized identifiers
  - Make security settings available through automation
  - Develop software with SCAP requirements in mind
- SCAP Content Producers
  - Develop security checklists in SCAP format and contribute them to the National Checklist Program
  - Participate in developing OVAL
- End-User Organizations
  - Acquire products and services that support SCAP
  - Use SCAP in organization-developed software, databases, etc.

# Existing SCAP Content

## National Vulnerability Database (NVD)

- http://nvd.nist.gov/download.cfm
- Data on over 43,000 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

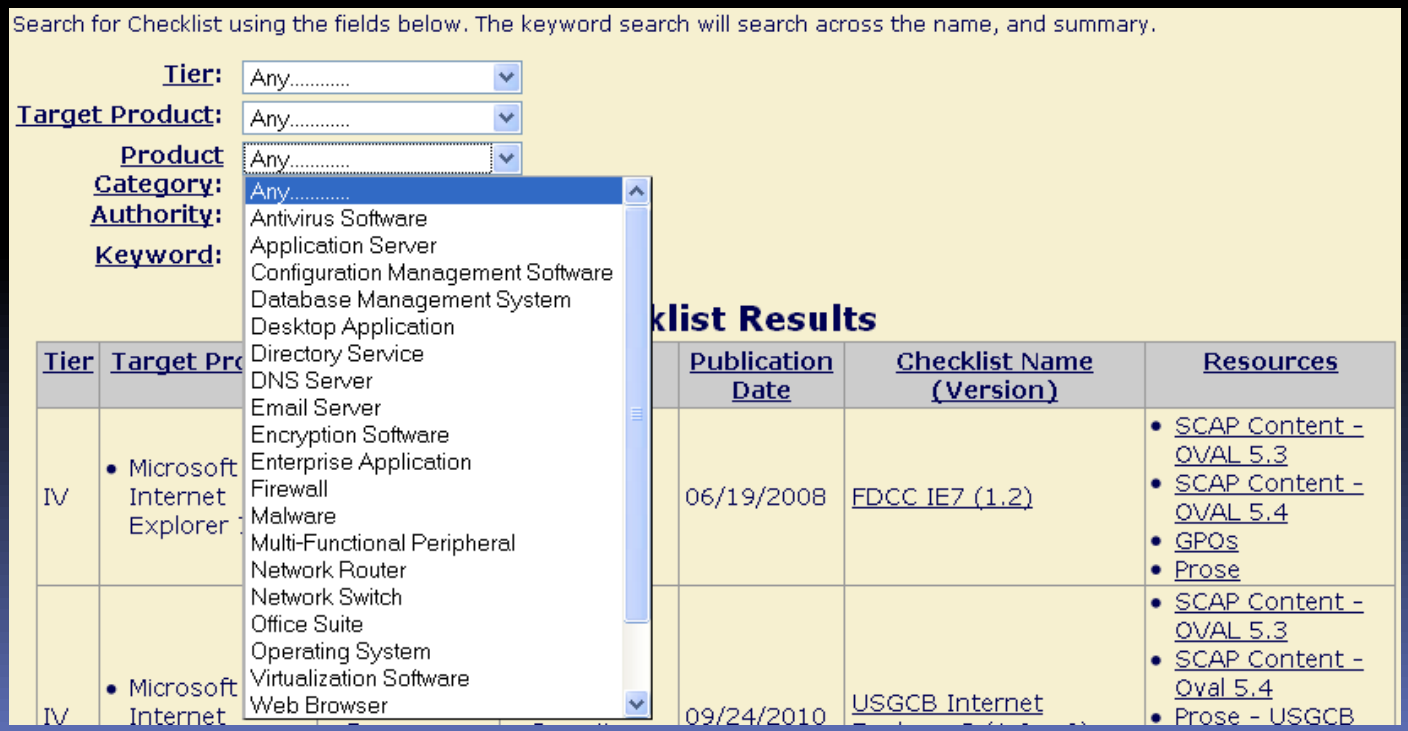
**Vulnerability Type** (View All)

Path Traversal (CWE-22)

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

# Existing SCAP Content

- 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, The Technical Specification for SCAP
  - Definitive technical specification for SCAP v 1.0
  - 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 1, 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

- Home page for SCAP

http://scap.nist.gov/revision/1.0/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

# SCAP Validation Program

- Independent laboratories test submitted products
  - Tests defined in NIST IR 7511, SCAP Validation Program Test Requirements
- NIST validates products based on the test results, then posts the validations
  - http://nvd.nist.gov/scapproducts.cfm
- Federal agencies have requirements to purchase SCAP-validated products
  - Details at http://nvd.nist.gov/scapproducts.cfm

# SCAP Validation Program Status

As of Sept. 24, 2010, 40 validated products from 30 vendors





















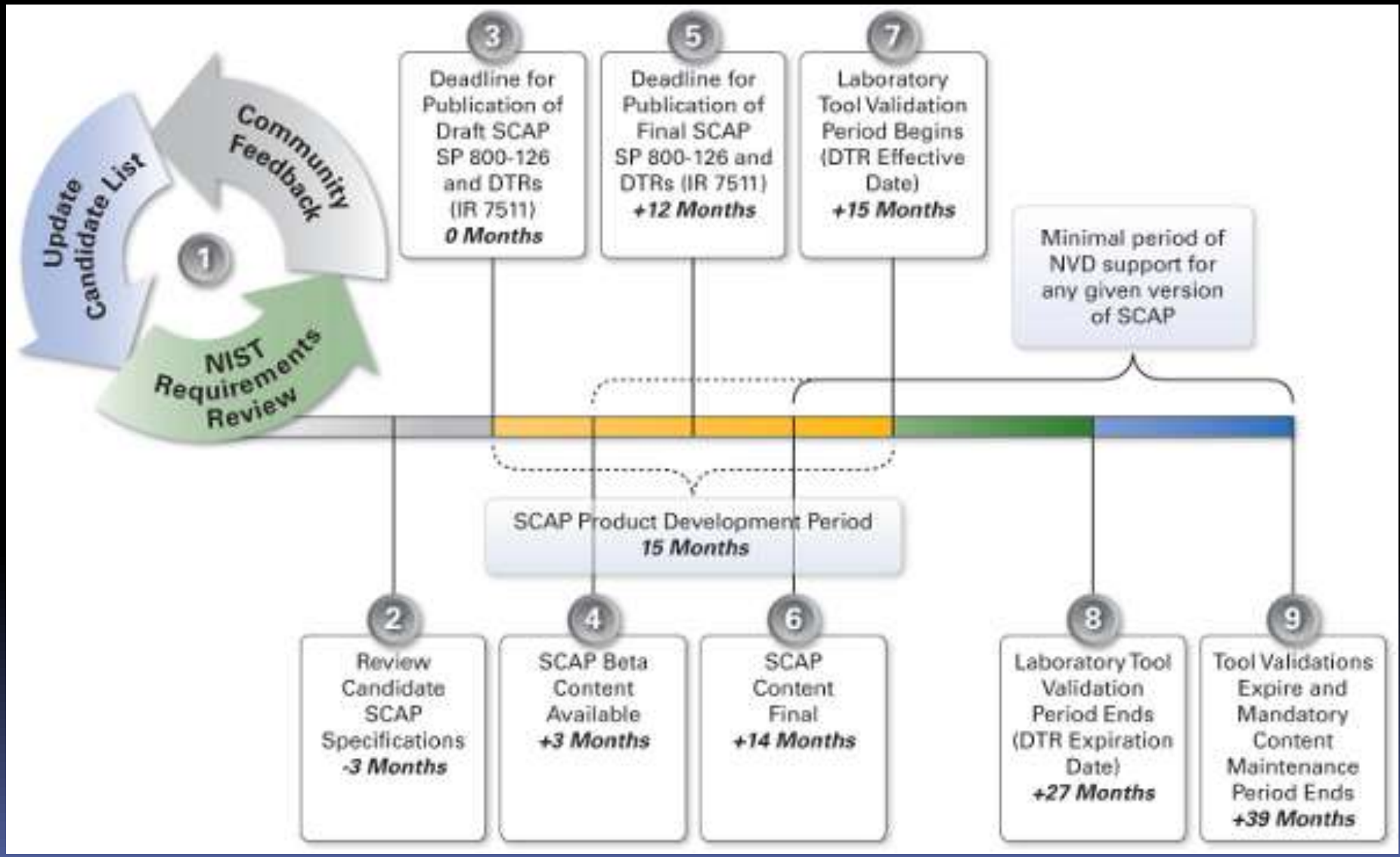









# SCAP Lifecycle




Reference: http://scap.nist.gov

# Current Lifecycle Iterations

- SCAP 1.0
  - Has been finalized
- SCAP 1.1
  - Second public draft of SP 800-126 released in May 2010
  - IR 7511 in development
  - Expect to finalize SCAP 1.1 in late 2010 (planned)
- SCAP 1.2
  - Developing and reviewing possible candidate specifications to include in SCAP 1.2

# SCAP 1.0 and Draft SCAP 1.1

| SCAP 1.0 | SCAP 1.1 |
|---|---|
| CVE | CVE |
| CCE 5 | CCE 5 |
| CPE 2.2 | CPE 2.2 |
| XCCDF 1.1.4 | XCCDF 1.1.4 |
| OVAL 5.3 and 5.4 | **OVAL 5.6** |
| CVSS 2.0 | CVSS 2.0 |
| | **OCIL 2.0** |

## Open Checklist Interactive Language (OCIL)

- Language for expressing security checks that require human interaction or that otherwise cannot be handled by OVAL
- Original draft specification released by MITRE for comment in August 2009

# Possible Future Additions

- Open Checklist Interactive Language (OCIL)
- Asset Reporting Format (ARF)
  - General security automation results reporting language
- Common Configuration Scoring System (CCSS)
  - Vulnerability measurement and scoring methodology for software security configuration issues

http://scap.nist.gov/emerging-specs/listing.html

# Recap

- The Need for Security Automation
- Introduction to SCAP
- Uses for SCAP
- SCAP Adoption
- SCAP Validation Program
- SCAP Lifecycle

# Recap

- The Need for Security Automation
- Introduction to SCAP
- Uses for SCAP
- SCAP Adoption
- SCAP Validation Program
- SCAP Lifecycle

http://scap.nist.gov/

# *Contact Information*

**Karen Scarfone**
Senior Security Engineer
703-401-1018 | karen.scarfone@g2-inc.com

# Remembering the Acronyms

| | |
|---|---|
| What IT systems do I have in my enterprise? | • CPE (Platforms) |
| What vulnerabilities do I need to worry about? | • CVE (Vulnerabilities) |
| What vulnerabilities do I need to worry about RIGHT NOW? | • CVSS (Scoring System) |
| How can I configure my systems more securely? | • CCE (Configurations) |
| How do I define a policy of secure configurations? | • XCCDF (Configuration Checklists) |
| How can I be sure my systems conform to policy? | • OVAL (Assessment Language) |


Reference: The MITRE Corporation, 2009