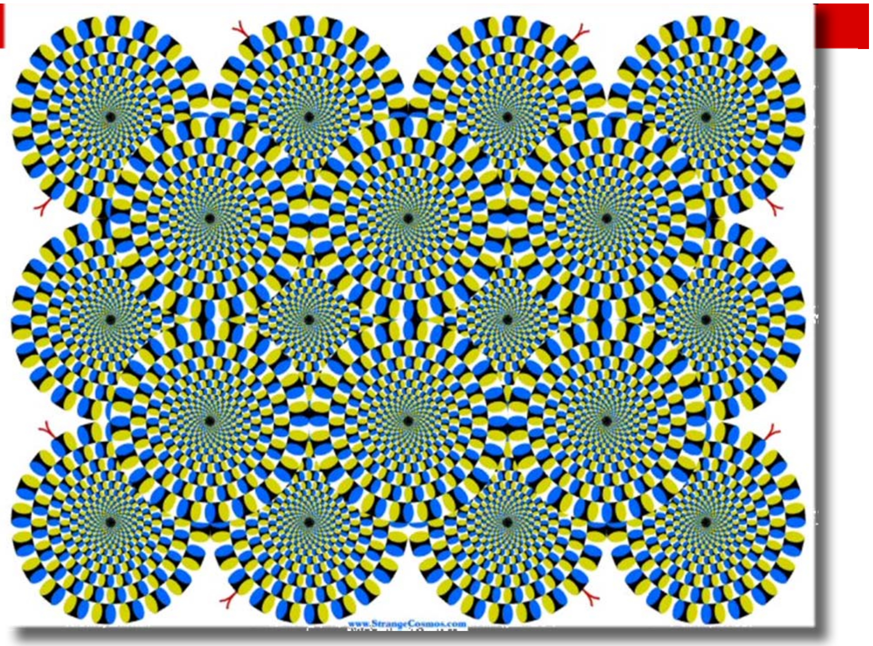


atsec CST: Security Content Automation Protocol (SCAP)

Fiona Pattinson, Steve Weingart

Federal Desktop Core Configuration Security Content Automation Protocol

Contents

- What is the problem?
- How is it tackled?
- The Office of Management & Budget mandate
- Federal Desktop Core Configuration standards
- Security Content Automation Protocol standards
- Security Content Automation capabilities
- The Testing and Validation Program

What is the problem?

- Many vulnerabilities are presented due to mis-configured systems
- An opportunity exists to strengthen U.S. Federal IT security by reducing opportunities for hackers to access and exploit government computer systems
- USGCB standards define common configuration criteria to standardize the configuration of various settings on their Windows XP, Vista and Windows 7, and Red Hat Linux Computers
- A companion standard, the Security Content Automation Protocol (SCAP), has also been created to define configurations, monitor compliance with the USGCB and assist with security posture assessment

How is it tackled?

- An opportunity to reduce vulnerabilities
  - Define checklists and standards
  - Mandate their use
  - Test products for compliance
    - Tools
    - A Validation Program

OMB mandate

- The United States Goverment Configuration Baseline is an OMB-mandated security configuration.
- The USGCB currently exists for Microsoft Windows Vista, XP, 7 and Red Hat Linux operating system software.
- The FDCC (USGCB Forerunner) was originally called for in a 22 March 2007 memorandum from OMB to all U.S. Federal agencies and department heads and a corresponding memorandum from OMB to all U.S. Federal agency and department Chief Information Officers
- Compliance was mandated by February 2008

FDCC = Federal Desktop Core Configuration

OMB = Office of Management and Budget

The USGCB standard

- The USGCB was developed (and is maintained) by the National Institute of Standards and Technology in collaboration with OMB, DHS, DISA, NSA, USAF, Microsoft and Red Hat with input from public comment
- The United States Air Force common security configurations for Windows XP were proposed as an early model on which standards could be developed.
- Released in 20 June 2008, FDCC Major Version 1.0 specified 674 settings. For example, "all wireless interfaces should be disabled"
- The latest version is USGCB Version 1.2

DHS = Department of Homeland Security

DISA = Defense Information Security Agency

NSA = National Security Agency

USAF = U.S. Air Force

http://web.nvd.nist.gov/view/ncp/repository

Checklists

- The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 1, is the repository of publicly available security checklists giving detailed low level guidance on setting the security configuration of OS and applications.
- NCP is migrating its repository of checklists to conform to SCAP
- Several checklists exist that are not formally part of the SCAP program (Which **only covers Windows XP, VISTA, 7 and Red Hat Linux to date**)
  - AIX
  - Solaris
  - HP Unix
  - Windows Server
  - MS Office
  - MS Sharepoint

http://web.nvd.nist.gov/view/ncp/repository

The SCAP standard

SCAP = Security Content Automation Protocol

- The Security Content Automation Protocol is a specification established by NIST for expressing and manipulating security data in standardized ways.
  - enumerates product names and vulnerabilities (both software flaws and configuration issues);
  - identifies the presence of vulnerabilities;
  - assigns severity scores to software flaw vulnerabilities.

- The SCAP specification defines what SCAP's components are and how they relate to each other within the context of SCAP
  - the SCAP specification does not define the SCAP components themselves; each component has its own standalone specification.

The SCAP standard

Pronounce SCAP

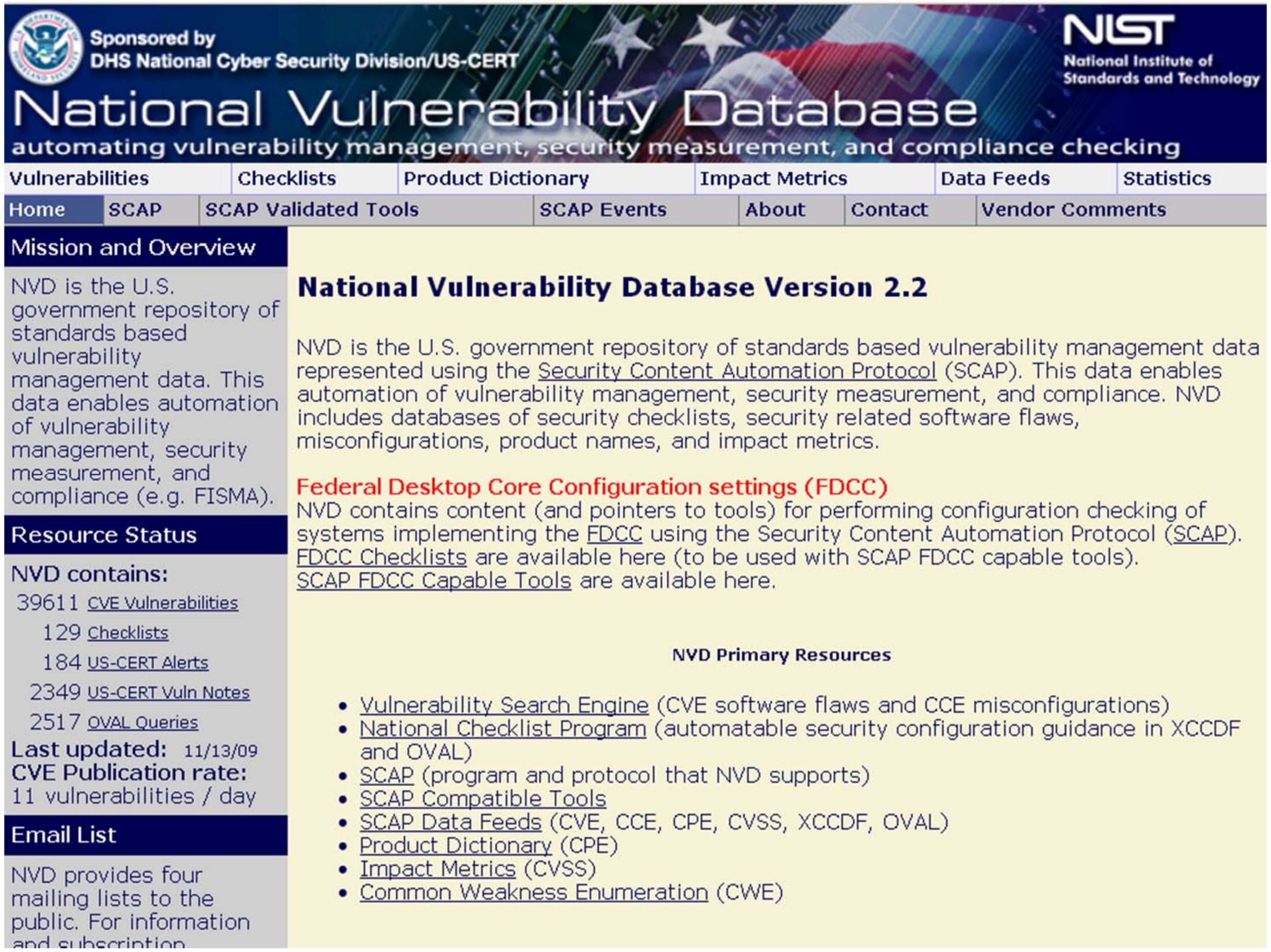
“Ess” “CAP”

- NIST provides SCAP content, such as vulnerability and product enumeration identifiers, through a repository supplied by the National Vulnerability Database (NVD).
- SCAP is to be used for automating activities such as security monitoring, vulnerability management, and security policy compliance evaluation reporting.
- The SCAP Standard is an interagency report.
  - IR 7511 version 3.04 is current
  - Give the test requirements

NIST. 2009, 'Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements.’

http://csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7511-Rev.%203.04

National vulnerability database


Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
Product Dictionary
Impact Metrics
Data Feeds
Statistics
Home
SCAP
SCAP Validated Tools
SCAP Events
About
Contact
Vendor Comments

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

39611 CVE Vulnerabilities
129 Checklists
184 US-CERT Alerts
2349 US-CERT Vuln Notes
2517 OVAL Queries

Last updated: 11/13/09

CVE Publication rate: 11 vulnerabilities / day

Email List

NVD provides four mailing lists to the public. For information and subscription

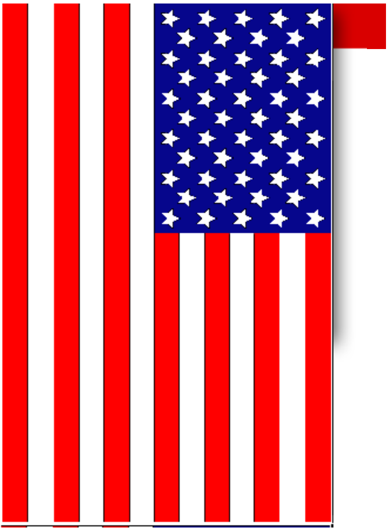
National Vulnerability Database Version 2.2

NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of security checklists, security related software flaws, misconfigurations, product names, and impact metrics.

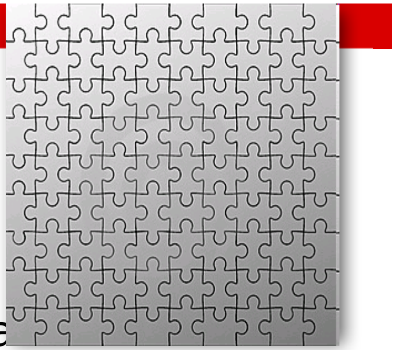
Federal Desktop Core Configuration settings (FDCC)
NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the FDCC using the Security Content Automation Protocol (SCAP). FDCC Checklists are available here (to be used with SCAP FDCC capable tools). SCAP FDCC Capable Tools are available here.

NVD Primary Resources

- Vulnerability Search Engine (CVE software flaws and CCE misconfigurations)
- National Checklist Program (automatable security configuration guidance in XCCDF and OVAL)
- SCAP (program and protocol that NVD supports)
- SCAP Compatible Tools
- SCAP Data Feeds (CVE, CCE, CPE, CVSS, XCCDF, OVAL)
- Product Dictionary (CPE)
- Impact Metrics (CVSS)
- Common Weakness Enumeration (CWE)



NVD at http://nvd.nist.gov/



SCAP components

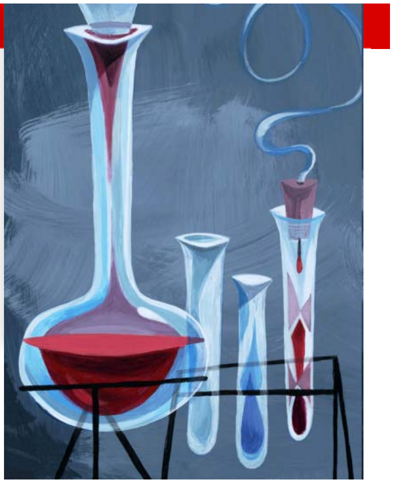
- The SCAP components were created and are maintained by severa entities, including the MITRE Corporation, the National Security Agency (NSA), and the Forum of Incident Response and Security Teams (FIRST).

- **Extensible Configuration Checklist Description Format (XCCDF)**
  - an XML specification for structured collections of security configuration rules used by operating system and application platforms
- **Open Vulnerability and Assessment Language (OVAL)**
  - an XML specification for exchanging technical details on how to check systems for security-related software flaws, configuration issues, and patches
- **Common Configuration Enumeration (CCE)**
  - a dictionary of names for software security configuration issues (e.g., access control settings, password policy settings)
- **Common Platform Enumeration (CPE)**
  - a naming convention for hardware, OS, and application products
- **Common Vulnerabilities and Exposures (CVE)**
  - a dictionary of names for publicly known security-related software flaws
- **Common Vulnerability Scoring System (CVSS)**
  - a method for classifying characteristics of software flaws and assigning severity scores based on these characteristics.

Current SCAP capability validation

- **Authenticated Configuration Scanner:**
  - audit and assess a target system to determine its compliance with a defined set of configuration requirements using target system logon privileges.

Testing and validation



- The NIST SCAP Validation Program is designed to test the ability of products to use the features and functionality available through SCAP and its components.
- Independent laboratories are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP)
- Accredited laboratories conduct the tests on IT security products and deliver the results to NIST
- The SCAP Validation Program then validates the product under test
- The validation certificates awarded to vendor products are publicly posted on the NIST SCAP Validated Products web page