National Institute of Standards and Technology
U.S. Department of Commerce

SCAP

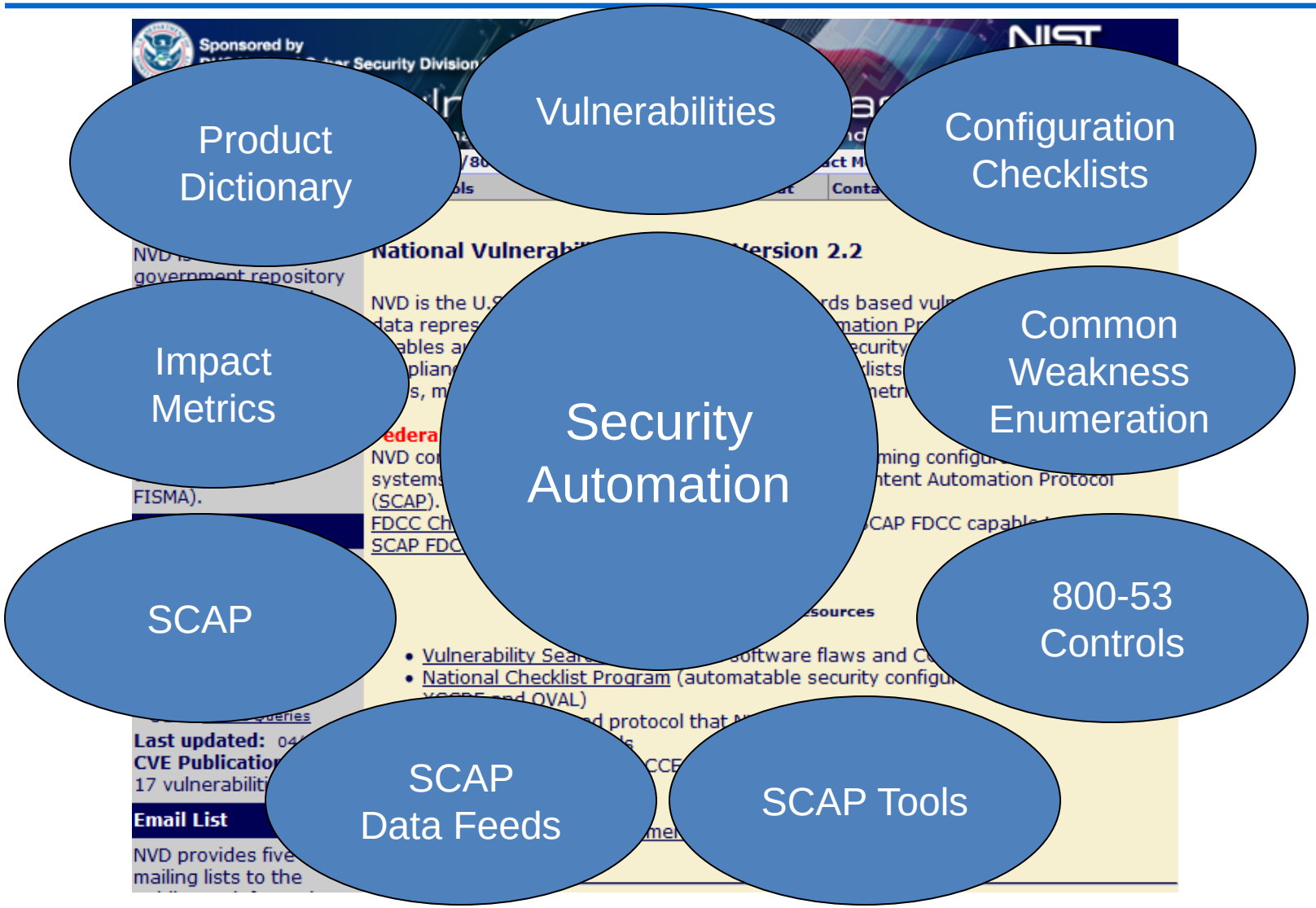
Security Automation and the National Vulnerability Database

Harold Booth
harold.booth@nist.gov

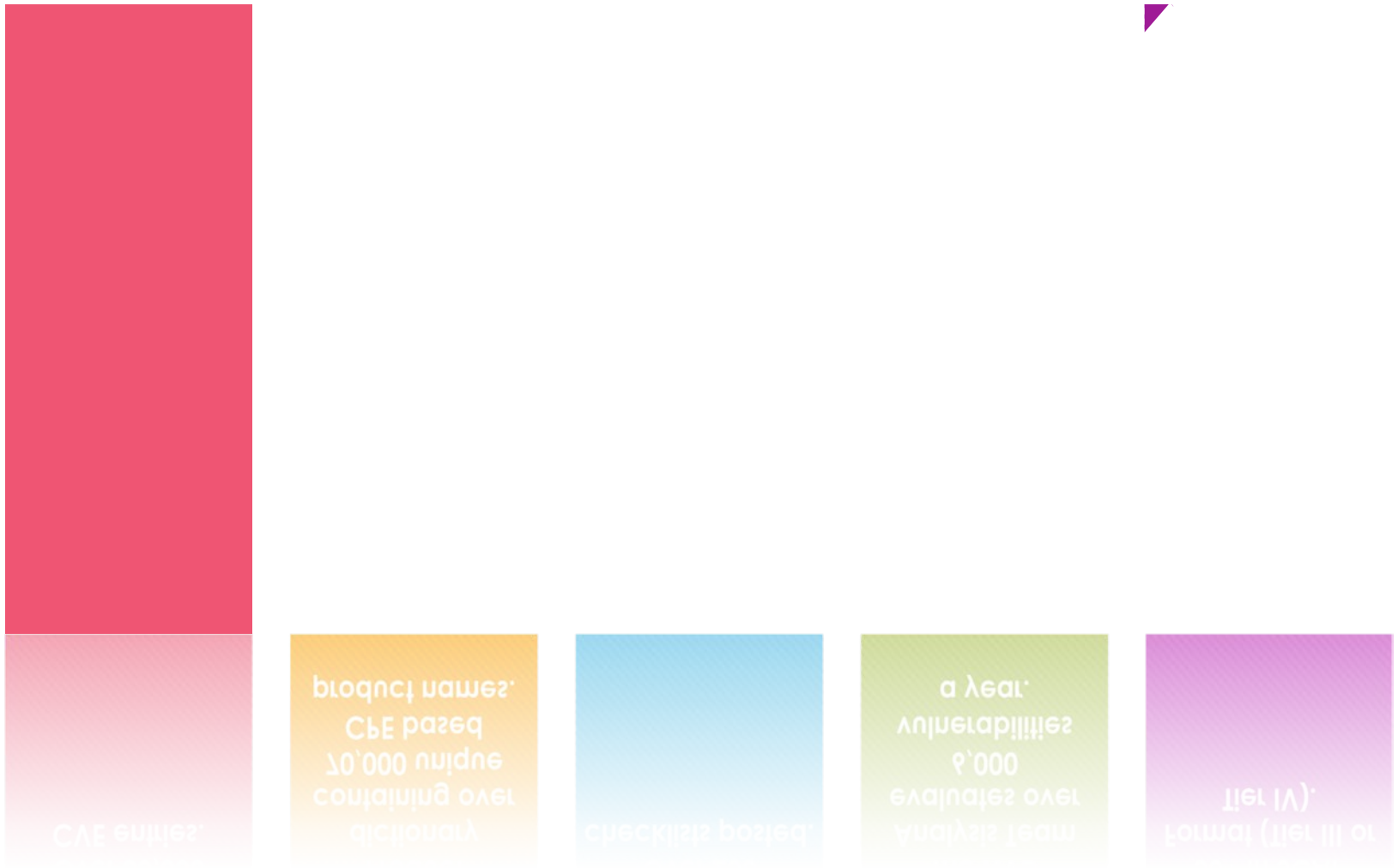
Agenda

- Introduction and Overview of the National Vulnerability Database (NVD)
- Introduction to NVD Resources
  - Vulnerabilities
  - Product Dictionary
  - National Checklist Program
- Security Content Automation Protocol (SCAP)
- Validated Products
- Use Cases

NVD: A Collection of Resources



NVD Overview



NVD Data Feeds

Vulnerabilities

Configuration to 800-53 Controls

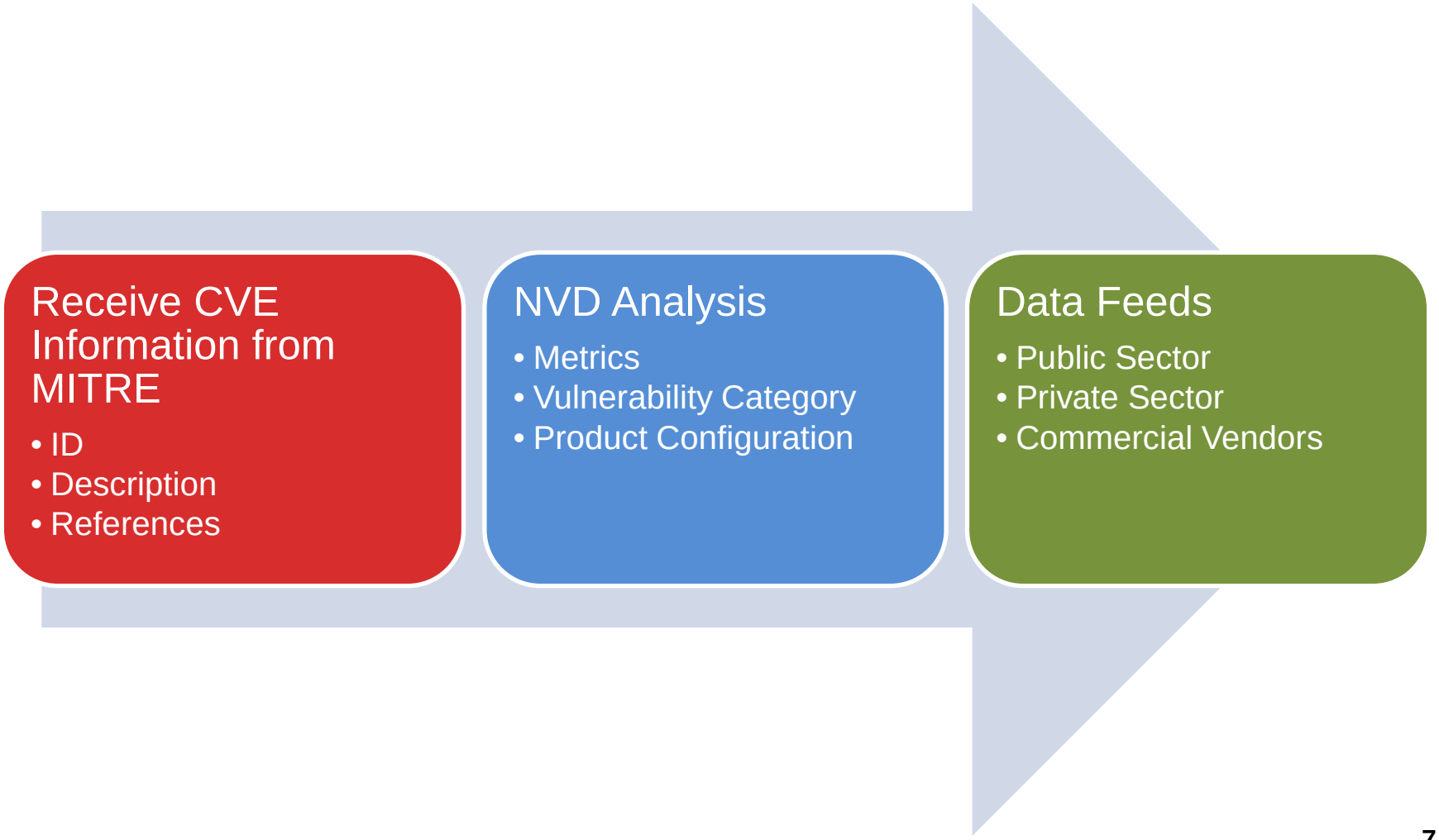
Checklists

Software Products

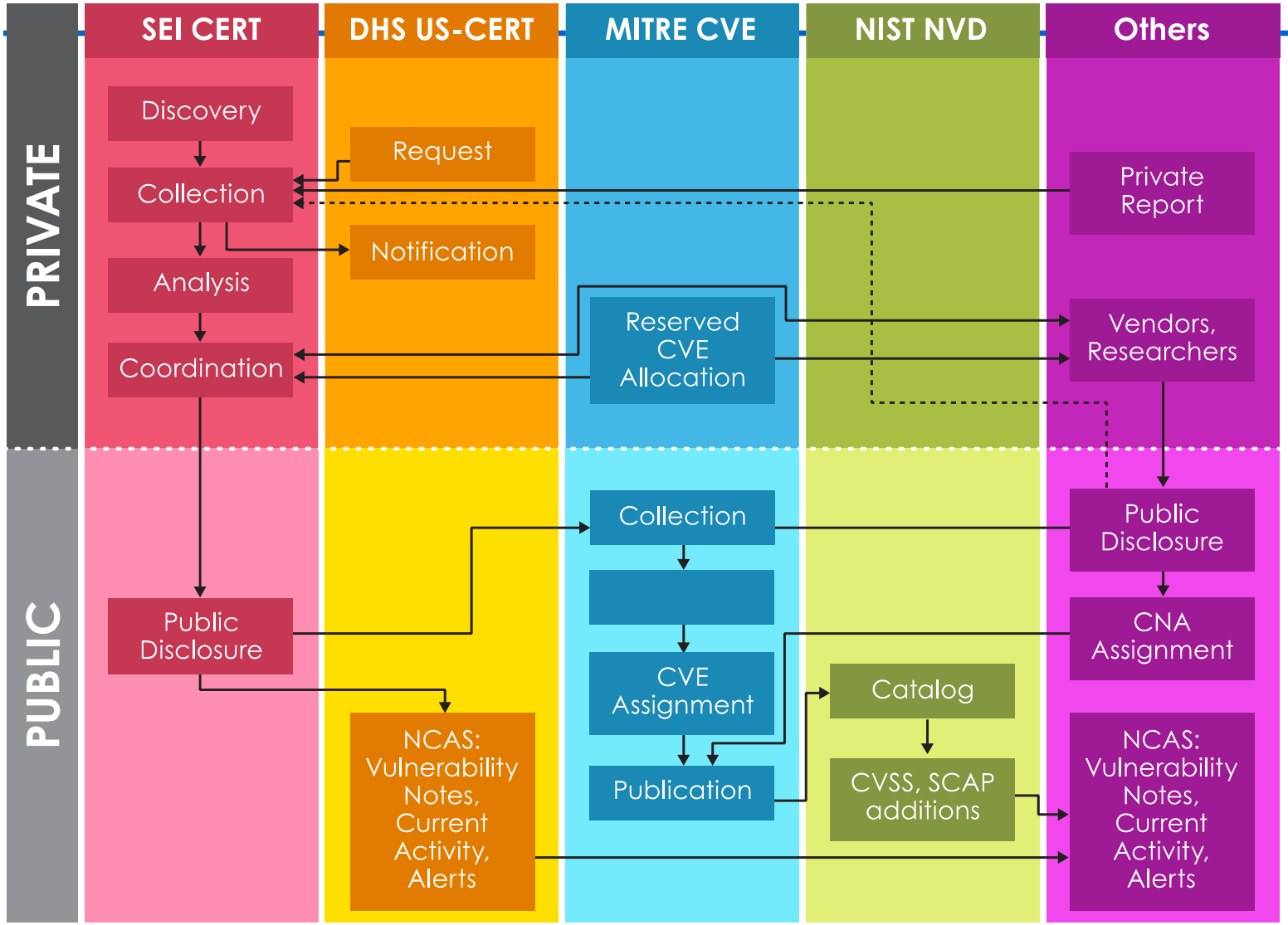
Common Vulnerabilities and Exposures (CVE)

- A dictionary of publicly known vulnerabilities
  - Predominately for, but not exclusive to, software used within the United States
  - MITRE maintains editorial control
    - Abstraction of Vulnerabilities
    - Duplication
- CVE is composed of:
  - Identifier => CVE-2013-1234
  - Description
  - References

National Vulnerability Database Role



CVE/NVD (US) Ecosystem



CVSS V2 Overview

- Common Vulnerability Scoring System (CVSS)
- A universal way to convey vulnerability severity and help determine urgency and priority of responses
- 20+ new vulnerabilities a day for organizations to prioritize and mitigate
- A set of metrics and formulas
- Solves problem of incompatible scoring systems
- Under the custodial care of FIRST CVSS-SIG
- Open, usable, and understandable by anyone
- Version 2 released in June 2007, adopted by SCAP

Base Metrics

Exploitability

Access Vector (AV)
- Local (L)
- Adjacent Network (A)
- Network (N)

Access Complexity (AC)
- Low (L)
- Medium (M)
- High (H)

Authentication (AU)
- None (N)
- Single (S)
- Multiple (M)

Impact

Confidentiality (C)
- None (N)
- Partial (P)
- Complete (C)

Integrity (I)
- None (N)
- Partial (P)
- Complete (C)

Availability (A)
- None (N)
- Partial (P)
- Complete (C)

Base Vector

Vector Format:

AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]
/C:[N,P,C]/I:[N,P,C]/A:[N,P,C]

Example:

AV:N/AC:L/Au:S/C:N/I:N/A:P

Temporal Metric

Exploitability (E)	Remediation Level (RL)	Report Confidence (RC)
• Unproven (U) • Functional (F) • High (H) • Not Defined (ND)	• Official Fix (OF) • Temporary Fix (TF) • Workaround (W) • Unavailable (U) • Not Defined (ND)	• Unconfirmed (UC) • Uncorroborated (UR) • Confirmed (C) • Not Defined (ND)

Environmental Metrics

Collateral Damage Potential (CDP)

- None (N)
- Low (L)
- Low-Medium (LM)
- Medium-High (MH)
- High (H)
- Not Defined (ND)

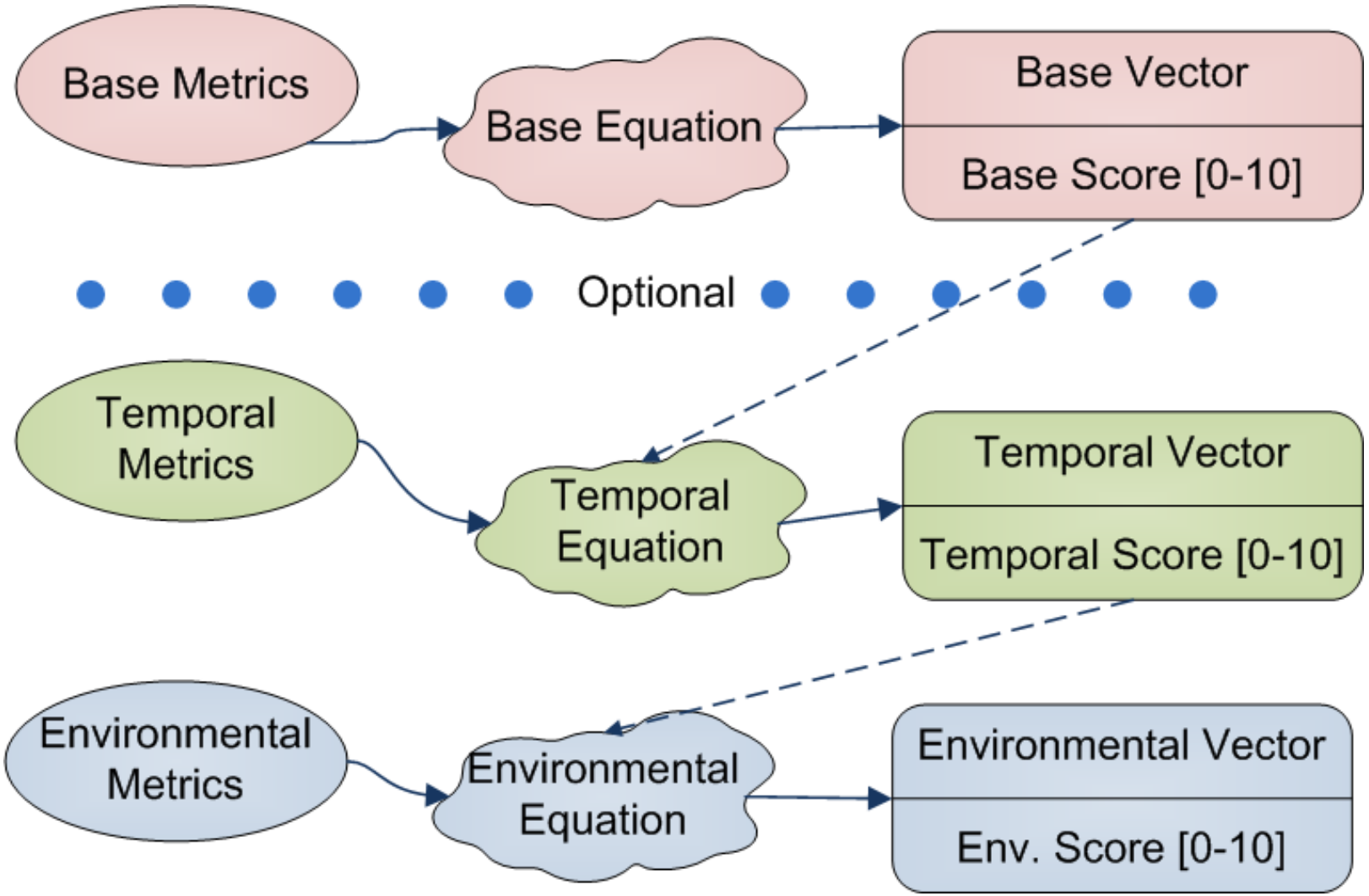
Target Distribution (TD)

- None (N)
- Low (L)
- Medium (M)
- High (H)
- Not Defined (ND)

Security Requirements

- **Confidentiality Requirement (CR)**
- **Integrity Requirement (IR)**
- **Availability Requirement (AR)**
- Low (L)
- Medium (M)
- High (H)
- Not Defined (ND)

Metrics and Scores



CVE Detail for NVD

Vulnerability Summary for CVE-2008-3013

Original release date: 09/11/2008

Last revised: 10/18/2011

Source: US-CERT/NIST

Overview

gdiplus.dll in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System, 2006, SQL Server 2000 Reporting Services SP2, SQL Server 200 remote attackers to execute arbitrary code via a malformed GIF i subsequent unknown labels, aka "GDI+ GIF Parsing Vulnerability.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C

Impact Subscore: 10.0

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable; Victim must voluntarily inte

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Provides administrator access, Allows complete co information; Allows disruption of service

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

US-CERT Technical Alert : TA08-253A

Name: TA08-253A

Hyperlink: http://www.us-cert.gov/cas/techalerts/TA

External Source : MISC

Name: http://www.zerodayinitiative.com/advisories/

Hyperlink: http://www.zerodayinitiative.com/advisori

External Source : MISC

Name: http://www.zerodayinitiative.com/advisories/

Hyperlink: http://www.zerodayinitiative.com/advisori

External Source : VUPEN

Name: ADV-2008-2696

Type: Advisory

Hyperlink: http://www.vupen.com/english/advisories

External Source : VUPEN

Name: ADV-2008-2520

Vulnerable software and versions

Configuration 1

OR

* cpe:/a:microsoft:ie:6:sp1
* cpe:/o:microsoft:windows_xp::sp2
* cpe:/o:microsoft:windows_xp::sp3
* cpe:/o:microsoft:windows_vista::gold
* cpe:/o:microsoft:windows_vista::sp2
* cpe:/o:microsoft:windows_server_2008:-
* cpe:/a:microsoft:office:xp:sp3
* cpe:/a:microsoft:office:2003:sp2
* cpe:/a:microsoft:office:2003:sp3
* cpe:/a:microsoft:office:2007::gold
* cpe:/a:microsoft:office:2007:sp1
* cpe:/a:microsoft:visio:2002:sp2
* cpe:/a:microsoft:powerpoint_viewer:2003
* cpe:/a:microsoft:works:8
* cpe:/a:microsoft:digital_image_suite:2006
* cpe:/a:microsoft:sql_server_reporting_services:2000:sp2
* cpe:/a:microsoft:sql_server:2005:sp2
* cpe:/a:microsoft:report_viewer:2005:sp1
* cpe:/a:microsoft:report_viewer:2008
* cpe:/a:microsoft:forefront_client_security:1.0

* Denotes Vulnerable Software

* Changes related to vulnerability configurations

Technical Details

Vulnerability Type (View All)

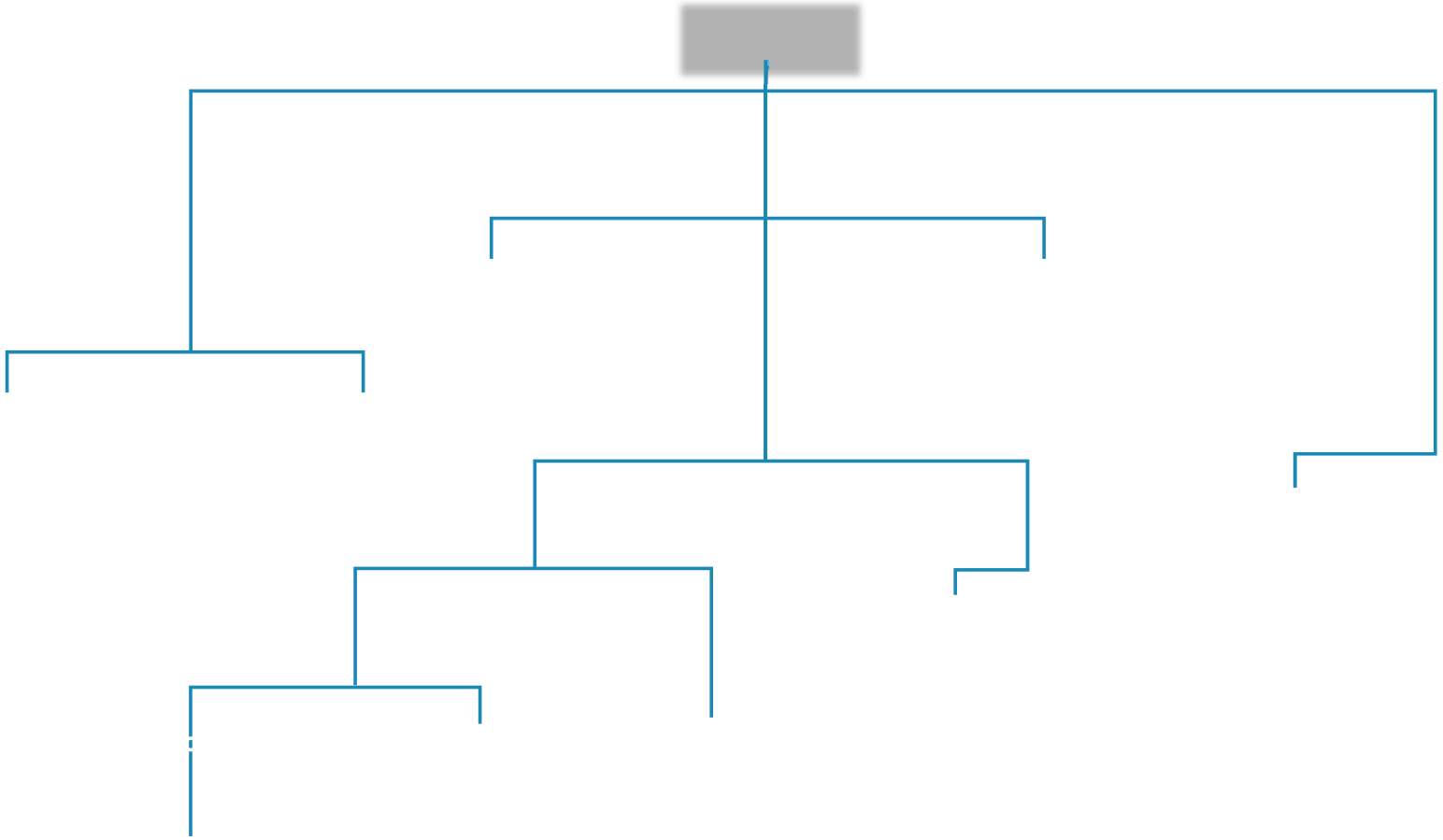
Resource Management Errors (CWE-399)

CVE Standard Vulnerability Entry: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3013

Disclaimer Notice & Privacy Statement / Security Notice
Send comments or suggestions to nvd@nist.gov
NIST is an Agency of the U.S. Department of Commerce
Full vulnerability listing
validate

CVE Detail for NVD - CWE

Portion of CWE Structure

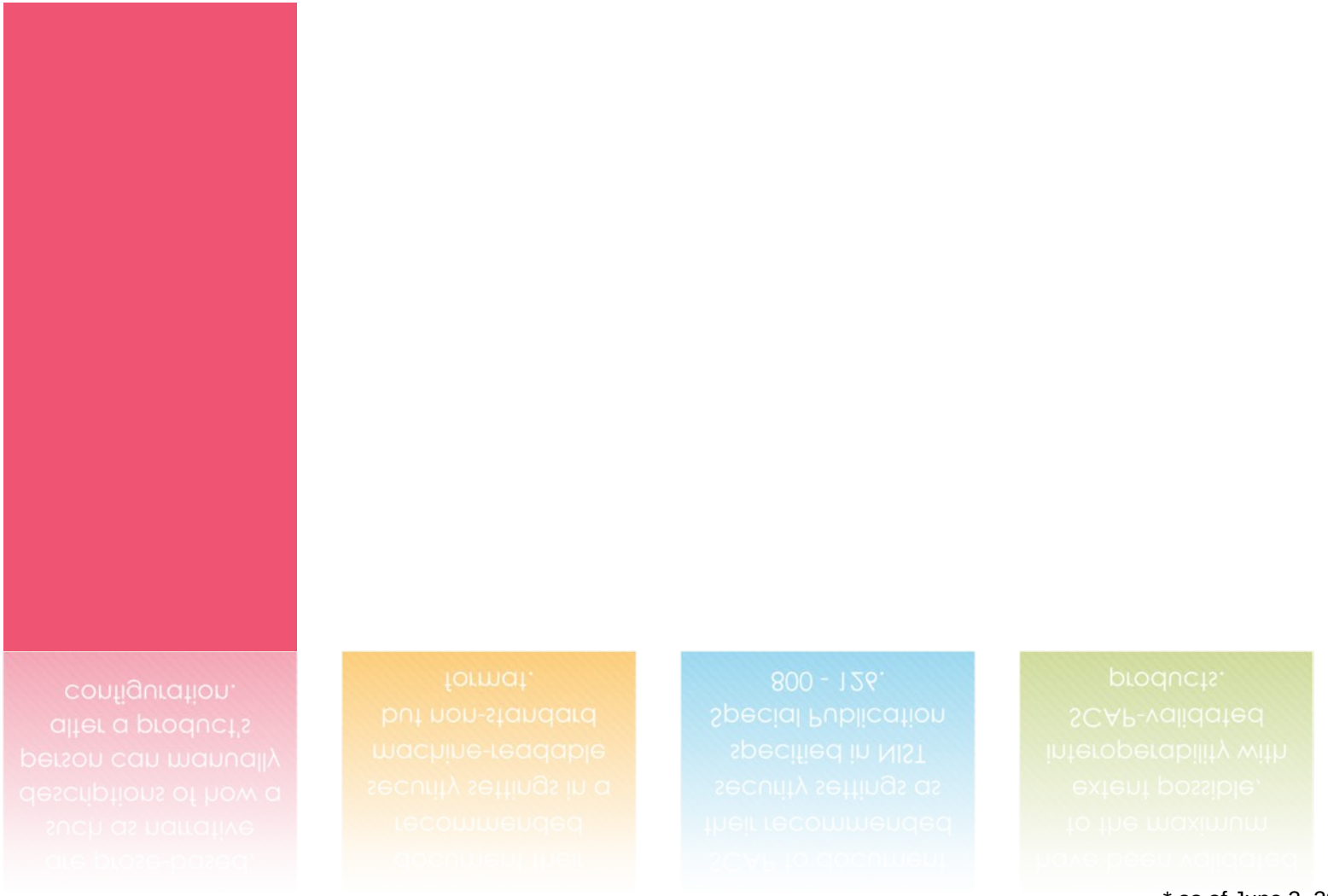


What is CPE?

- Structure naming scheme for information technology systems, software, and packages
- Includes formal name format, method for checking names against a system, and a description format for binding text and tests to a name
- The Official Common Platform Enumeration (CPE) Dictionary
  - http://nvd.nist.gov/cpe.cfm

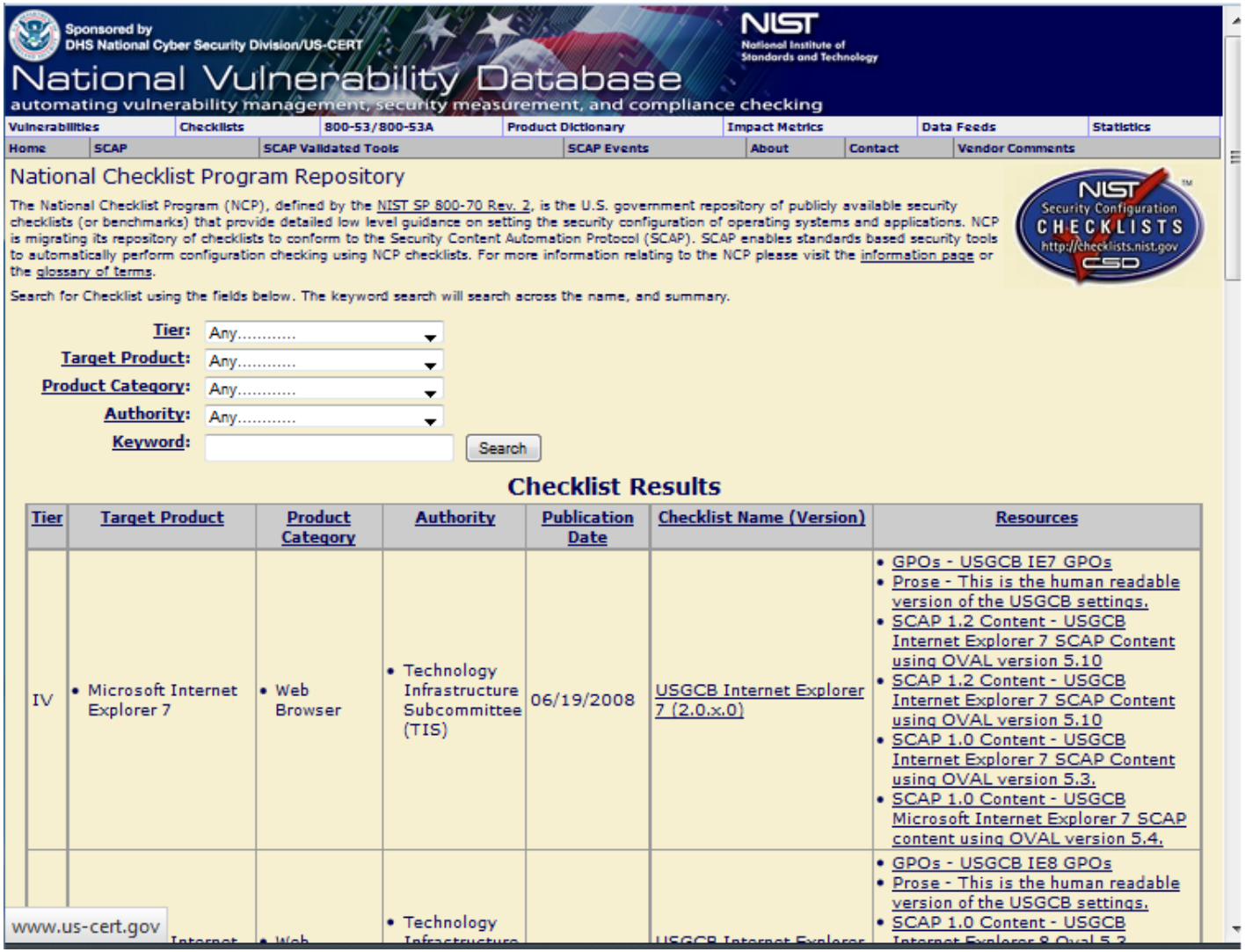
The National Checklist Program (NCP)

Project website: http://checklists.nist.gov



* as of June 3, 2013

The National Checklist Program (NCP)

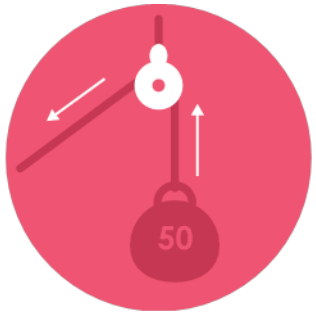


What is SCAP?

Security Content Automation Protocol

- Brings existing specifications together to provide a standardized approach for maintaining the security of enterprise systems
- Provides a means to identify, express and measure security data in standardized ways.
- Currently in 3rd revision – SCAP 1.2
  - Defined by Special Publication (SP) 800-126 Revision 2
  - SP 800-117 Revision 1
  - Project website: http://scap.nist.gov

Why should I use SCAP?



Minimize Effort

Increase Interoperability

Economy of Scale and Reuse

Speed

How Does SCAP Work?

Languages

Means of providing instructions

- Community developed
- Machine readable XML
- Reporting
- Representing security checklists
- Detecting machine state

Metrics

Risk scoring framework

- Community developed
- Transparent
- Metrics
  - Base
  - Temporal
  - Environmental

Enumerations

Convention for identifying and naming

- Community developed
- Product names
- Vulnerabilities
- Configuration settings

Integrity

Conventions for applying existing and emerging XML signature standards and best practices to sign and verify content

What are SCAP Validated Products?

- Products validated by the SCAP Validation Program
- The SCAP Validation Program
  - Provides product conformance testing for Security Content Automation Protocol (SCAP)
  - Provides end users with assurance that SCAP validated tools conform to SCAP and should be capable of processing well-formed SCAP expressed checklists

SCAP 1.0 Validated Products

http://nvd.nist.gov/scapproducts.cfm

As of April 18, 2013

How do I use SCAP Validated Products?

- End users purchasing a tool from the validated products list has assurance that the product has met the test requirements defined in NIST IR 7511 and should process SCAP expressed checklists.
- http://nvd.nist.gov/scapproducts.cfm

Use Case: Configuration Assessment

http://nvd.nist.gov/scapproducts.cfm

Authenticated Configuration Scanner

http://usgcb.nist.gov

http://checklists.nist.gov

Use Case: Configuration Assessment

```
<!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
<xccdf:Rule id="xccdf_gov.nist_rule_account_lockout_duration" selected="false" weight="10.0">
  <xccdf:title>Account Lockout Duration</xccdf:title>
  <xccdf:description>This value specifies how long the user account should be locked out. This
  <xccdf:reference>
    <dc:type>GPO</dc:type>
    <dc:source>Computer Configuration\Windows Settings\Security Settings\Account Policies\Accou
  </xccdf:reference>
  <xccdf:ident system="http://cce.mitre.org">CCE-9308-8</xccdf:ident>
  <xccdf:check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <xccdf:check-export export-name="oval:gov.nist.usgcb.windowsseven:var:23" value-id="xccdf_g
    <xccdf:check-content-ref href="USGCB-Windows-7-oval.xml" name="oval:gov.nist.usgcb.windowss
  </xccdf:check>
</xccdf:Rule>
```

- SCAP 1.2 Datastream
- Windows 7 USGCB Content
  - CCE-9308-8

Use Case: Configuration Assessment

```
<entry id="CCE-9308-8">
    <config:cce-id>CCE-9308-8</config:cce-id>
    <config:published-datetime>2010-09-24T16:44:34.730Z</config:published-d
    <config:last-modified-datetime>2012-05-25T03:59:21.197Z</config:last-mo
    <config:summary>The 'Account lockout duration' setting should be config
    <scap-core:control-mappings>
        <scap-core:control-mapping last-modified="2011-04-18T20:18:49.687Z"
            <scap-core:mapping published="2011-04-18T20:18:49.687Z">AC-7</s
        </scap-core:control-mapping>
    </scap-core:control-mappings>
</entry>
```

- CCE-to-800-53 Mapping
  - CCE-9308-8
  - AC-7 From NIST SP 800-53 Revision 3

Use Case: Configuration Assessment

```
<control-class>Technical</control-class>
<family>Access Control</family>
<number>AC-7</number>
<title>Unsuccessful Login Attempts</title>
<priority>P2</priority>
<description>
    <ns2:div>
        <ns2:p class="align_left">The information system:</ns2:p>
        <ns2:p class="align_left"/>
    </ns2:div>
</description>
<supplemental-guidance>
    <ns2:div>
        <ns2:p class="align_left">Due to the potential for denial of service, au
    </ns2:div>
</supplemental-guidance>
<control-enhancements>
    <control-enhancement sequence="1">
```

- 800-53 Controls File
  - AC-7

Use Case: Vulnerability Management

CVE 2012-3544

Search CVE and CCE Vulnerability Database

(Advanced Search)

Keyword search: Search

Try a product or vendor name

Try a CVE standard vulnerability name or OVAL query

Only vulnerabilities that match ALL keywords will be returned

Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

- ○ Search All
- ◉ Search Last 3 Months
- ○ Search Last 3 Years

Use Case: Vulnerability Management

Vulnerability Summary for CVE-2012-3544

Original release date: 06/01/2013

Last revised: 06/03/2013

Source: US-CERT/NIST

Overview

Apache Tomcat 6.x before 6.0.37 and 7.x before 7.0.30 does not properly handle cause a denial of service by streaming data.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 5.0 (MEDIUM) (AV:N/AC:L/Au:N/C:N/I:N/A:P) (legend)

Impact Subscore: 2.9

Exploitability Subscore: 10.0

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Low

Authentication: Not required to exploit

Impact Type: Allows disruption of serviceUnknown

Use Case: Vulnerability Management

External Source : CONFIRM

Name: http://tomcat.apache.org/security-7.html

Type: Advisory

Hyperlink: http://tomcat.apache.org/security-7.html

External Source : CONFIRM

Name: http://tomcat.apache.org/security-6.html

Type: Advisory

Hyperlink: http://tomcat.apache.org/security-6.html

Use Case: Vulnerability Management

Vulnerable software and versions

- Configuration 1
  - OR
    - * cpe:/a:apache:tomcat:6.0.15
    - * cpe:/a:apache:tomcat:6.0.30
    - * cpe:/a:apache:tomcat:6.0
    - * cpe:/a:apache:tomcat:6.0.14
    - * cpe:/a:apache:tomcat:6.0.36
    - * cpe:/a:apache:tomcat:6.0.6
    - * cpe:/a:apache:tomcat:6.0.7
    - * cpe:/a:apache:tomcat:6.0.9:beta
    - * cpe:/a:apache:tomcat:6.0.8
    - * cpe:/a:apache:tomcat:6.0.9
    - * cpe:/a:apache:tomcat:6.0.8:alpha
    - * cpe:/a:apache:tomcat:6.0.35
    - * cpe:/a:apache:tomcat:6.0.7:beta
    - * cpe:/a:apache:tomcat:6.0.29
    - * cpe:/a:apache:tomcat:6.0.7:alpha
    - * cpe:/a:apache:tomcat:6.0.6:alpha
    - * cpe:/a:apache:tomcat:6.0.33

Future of NVD

Resources and Websites

- **NVD Homepage**
  - http://nvd.nist.gov
- **National Checklist Program**
  - http://checklists.nist.gov
- **SCAP Homepage**
  - http://scap.nist.gov
- **SCAP Validated Products**
  - http://nvd.nist.gov/scapproducts.cfm
- **NIST Computer Security Resource Center (CRSC) Documents**
  - http://csrc.nist.gov/publications/PubsSPs.html
  - http://csrc.nist.gov/publications/PubsNISTIRs.html

Questions

Harold Booth
harold.booth@nist.gov

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology