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

SCAP™

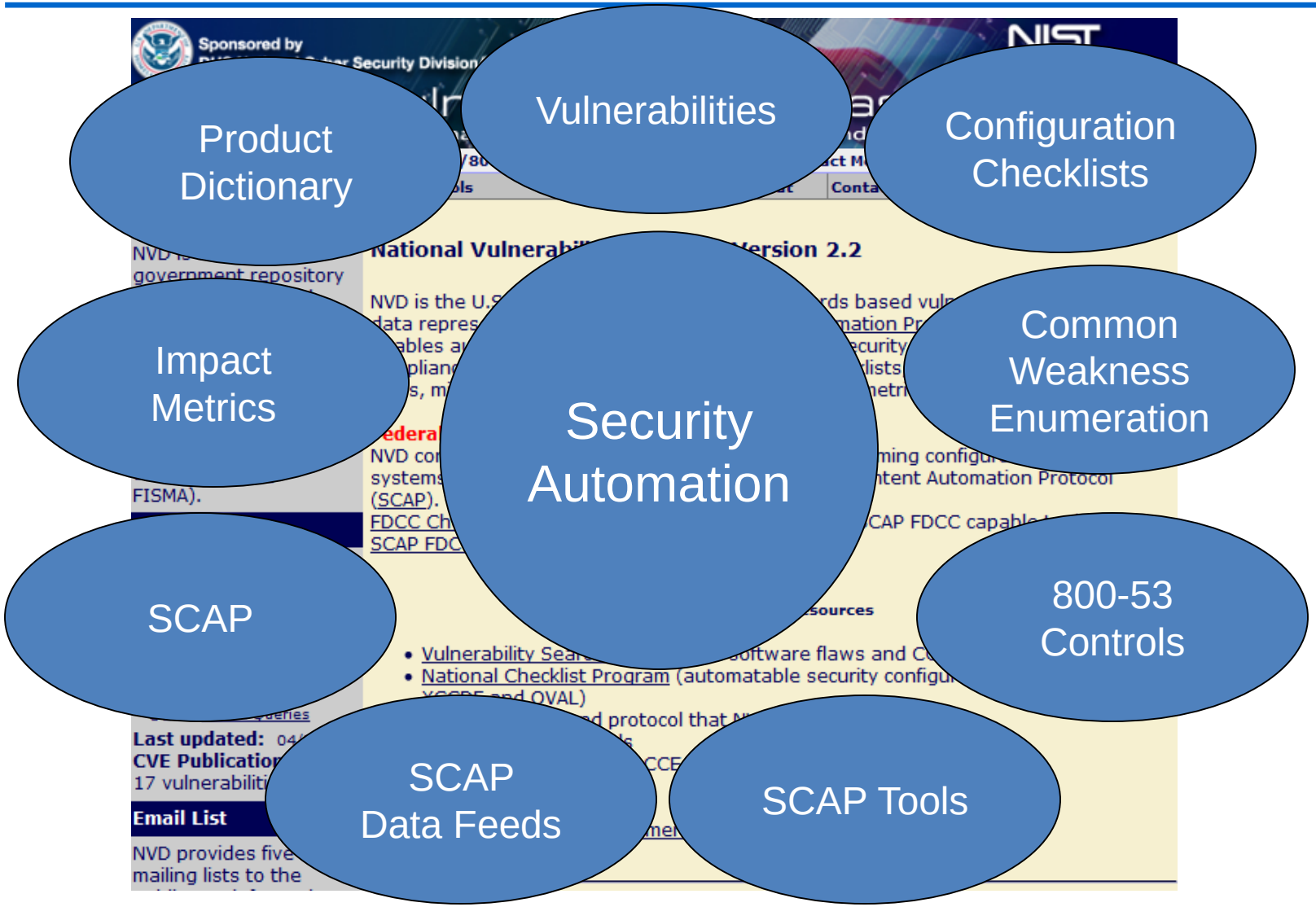
The National Vulnerability Database

Harold Booth

Agenda

- Introduction and Overview of the National Vulnerability Database (NVD)
- Introduction to NVD Resources
- CVE
- CVSS
- Vulnerability Taxonomy
- Q&A - Feedback

NVD: A Collection of Resources



NVD Overview

Vulnerabilities	Product Names	Checklists	New Vulnerabilities	SCAP Checklists
				
72,000+	105,000+	290+	6,000+	80+
• Over 72,000 CVE entries	• Product dictionary containing over 105,000 unique CPE based product names	• Over 290 Checklists posted.	• The NVD Analysis Team evaluates over 6,000 vulnerabilities a year	• 80+ in SCAP Format (Tier III or Tier IV).

NVD Data Feeds

Vulnerabilities

Configuration to 800-53 Controls

Checklists

Software Products

Security Content Automation Protocol (SCAP)

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

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

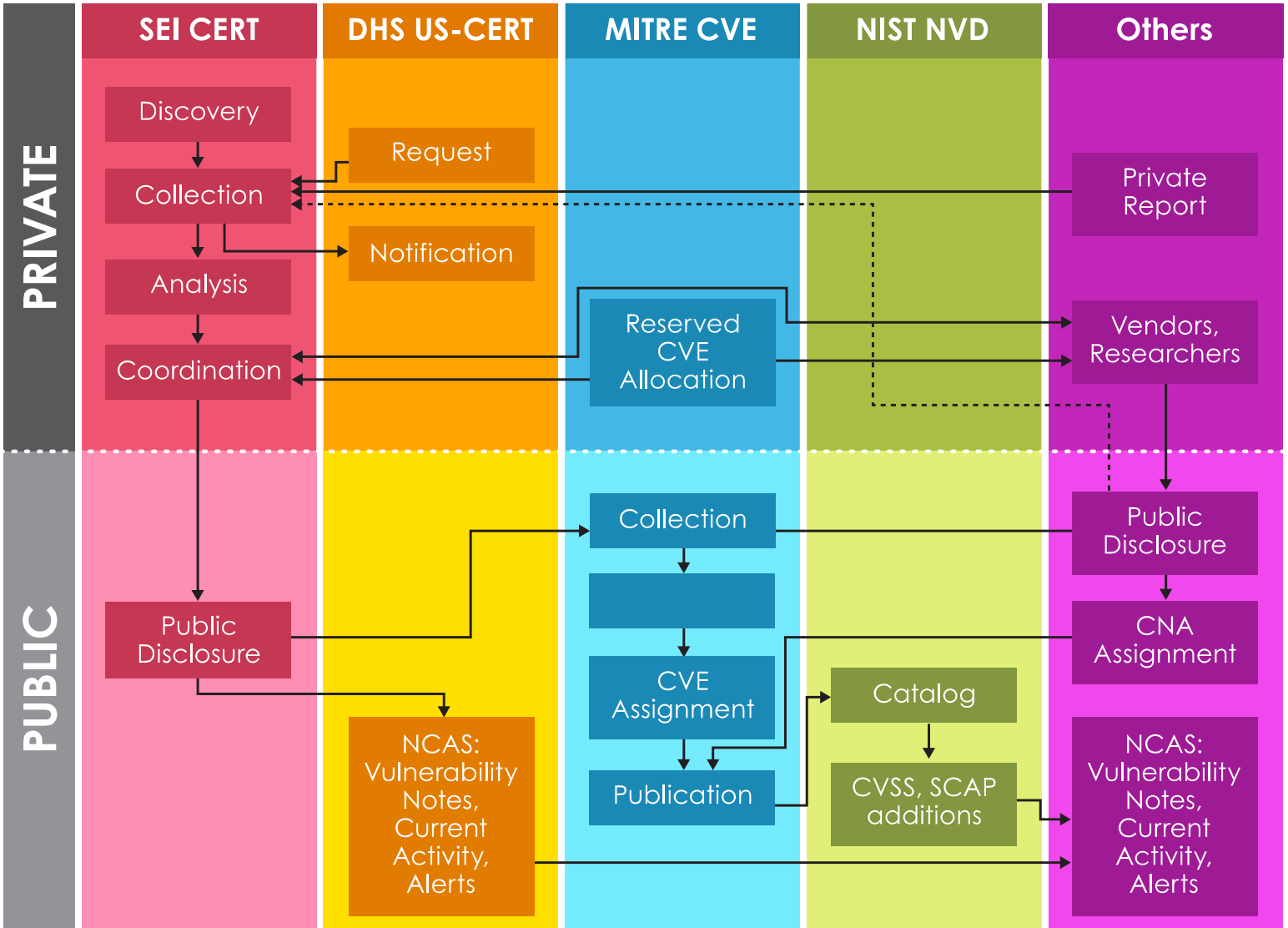
What is CPE?

- 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

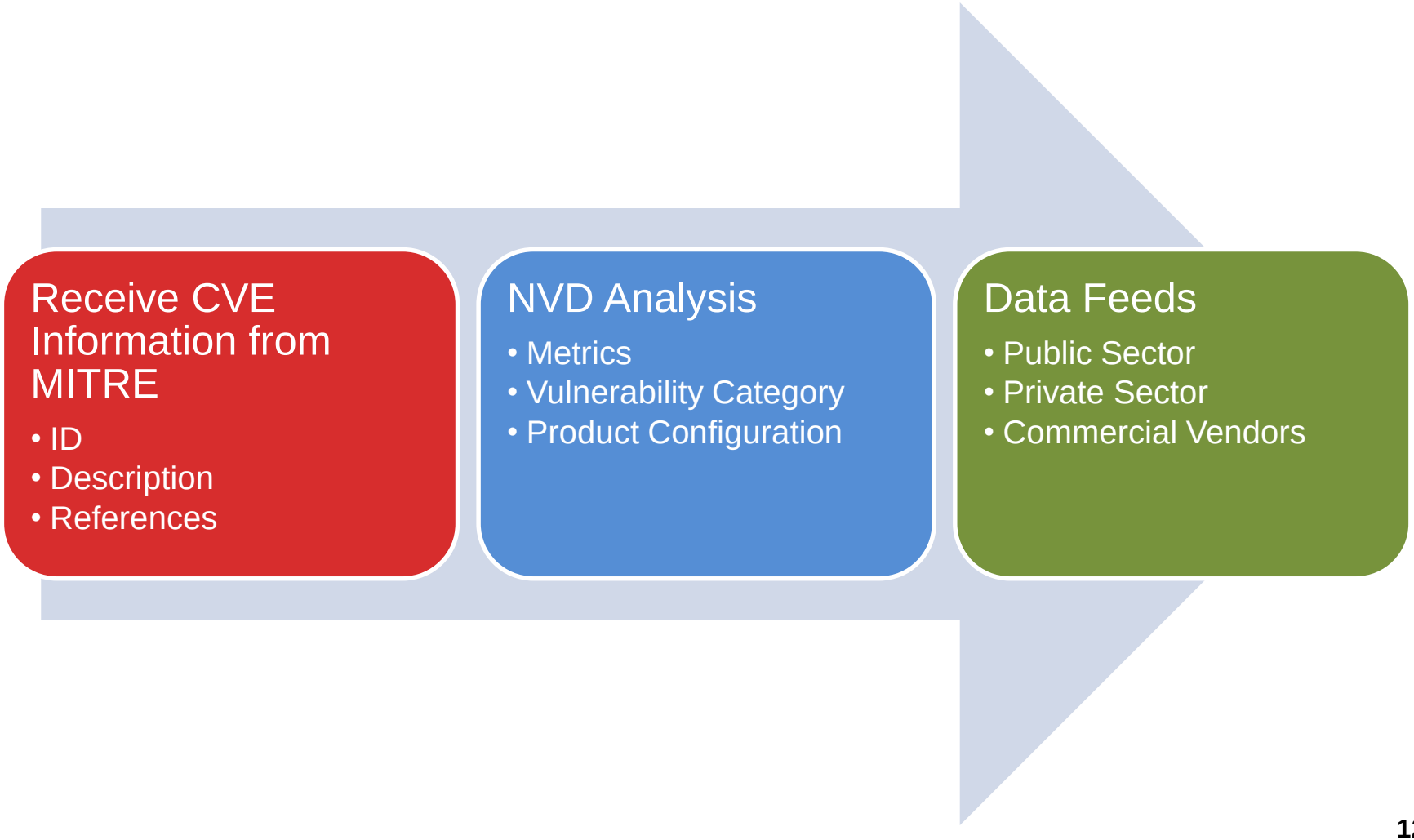
Common Vulnerabilities and Exposures (CVE)

- 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

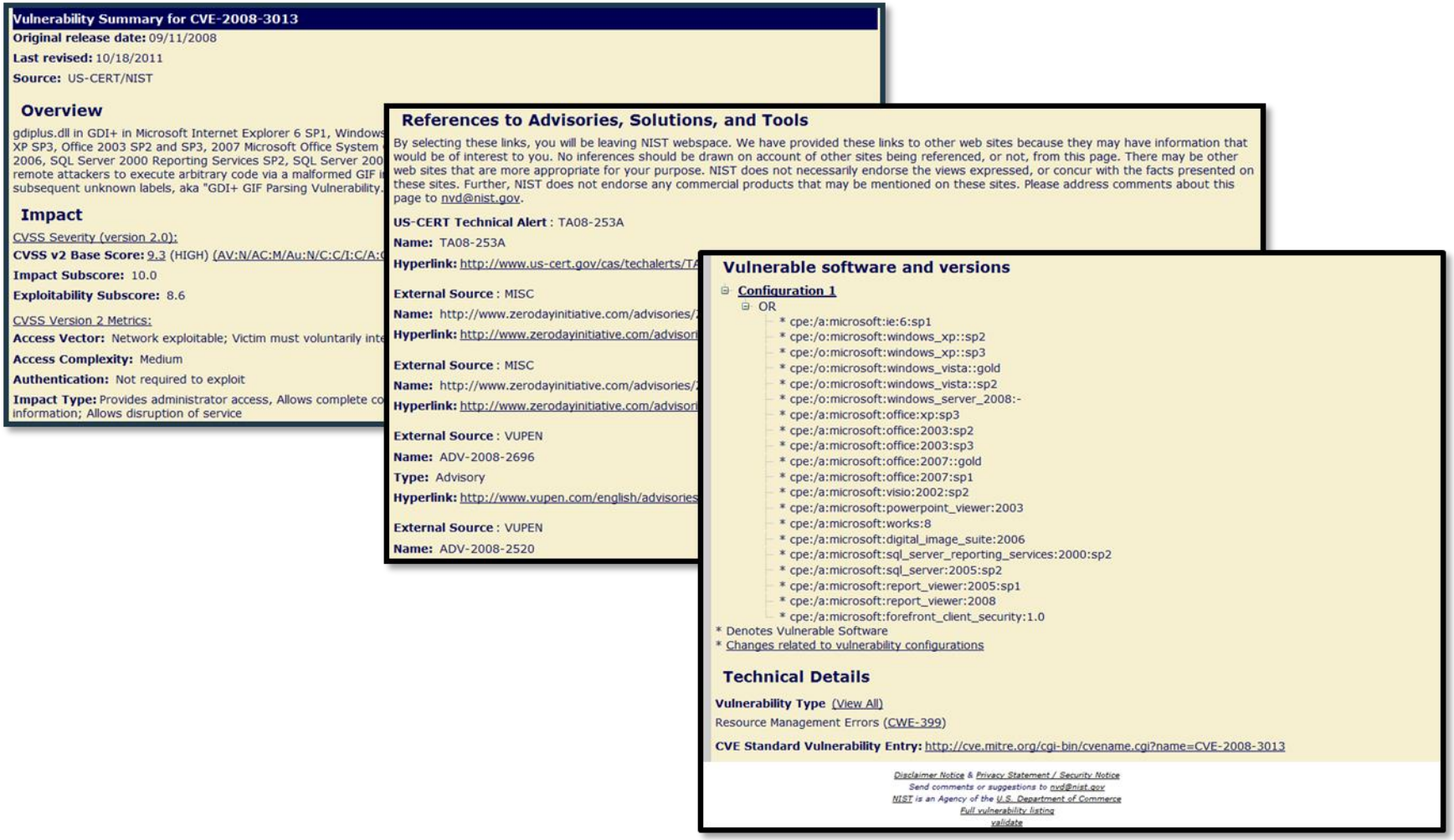
CVE/NVD (US) Ecosystem



National Vulnerability Database Role



CVE Detail for NVD



CVSS 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
- Version 3 released in June 2015

CVSS v2.0 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)

CVSS v2.0 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

CVSS v2.0 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)

CVSS v2.0 Environmental Metrics

Collateral Damage Potential (CDP)

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

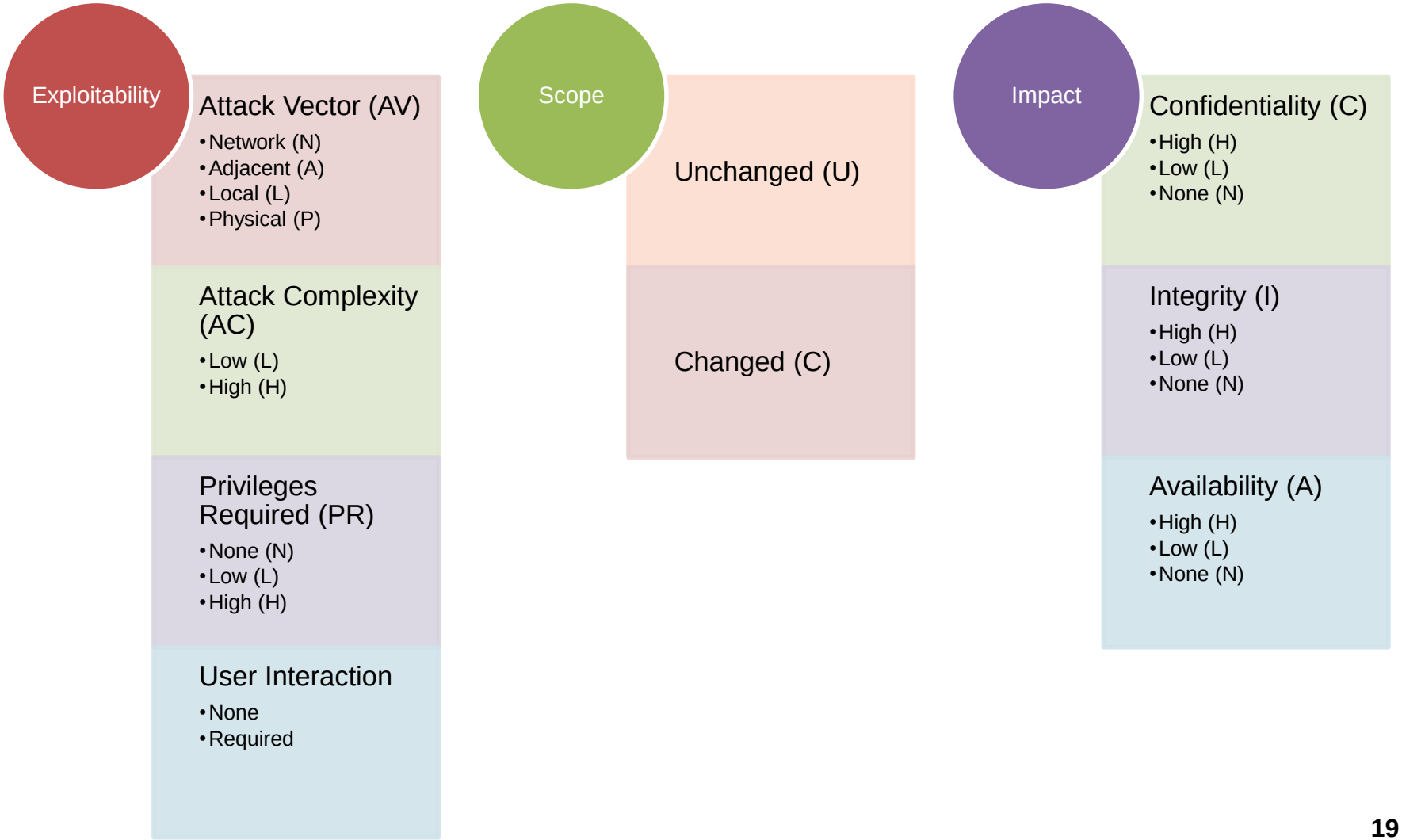
Target Distribution (TD)

- 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)

CVSS v3.0 Base Metrics



CVSS v3.0 Base Vector

Vector Format:

CVSS:3.0/AV:[N,A,L,P]/AC:[L,H]
/PR:[N,L,H]/UI:[N,R]/S:[U,C]
/C:[H,L,N]/I:[H,L,N]/A:[H,L,N]

Example:

CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:L
/I:L/A:N

CVSS v3.0 Temporal Metric

Exploit Code Maturity (E)	Remediation Level (RL)	Report Confidence (RC)
• Not Defined (X) • High (H) • Functional (F) • Proof-of-Concept (P) • Unproven (U)	• Not Defined (X) • Unavailable (U) • Workaround (W) • Temporary Fix (TF) • Official Fix (OF)	• Not Defined (X) • Confirmed (C) • Reasonable (R) • Unknown (U)

CVSS v3.0 Environmental Metrics

Security Requirements

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

Modified Based Metrics

- **Modified Attack Vector (MAV)**
- **Modified Attack Complexity (MAC)**
- **Modified Privileges Required (MPR)**
- **Modified User Interaction (MUI)**
- **Modified Scope (MS)**
- **Modified Confidentiality (MC)**
- **Modified Integrity (MI)**
- **Modified Availability (MA)**
  - Not Defined (X)
  - Same as equivalent Base Metric

Vulnerability Taxonomy

- Evaluate vulnerabilities only once
  - Generate CVSS v2.0 & v3.0 scores
- Common vocabulary
- Improve Automation
- Support sharing across regional and linguistic boundaries
- Currently in Research and Development phase

Questions

- What information is valuable to your organization when evaluating vulnerabilities?
- What is the desired level of automation?

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