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

- Product Dictionary
- Vulnerabilities
- Configuration Checklists
- Impact Metrics
- Security Automation
- Common Weakness Enumeration
- SCAP
- SCAP Data Feeds
- SCAP Tools
- 800-53 Controls

NVD is the U.S. federal government repository of vulnerabilities and other system security flaws, as well as software and configuration settings. NVD is the foundation for the Federal Desktop Configuration Computing (FDCC) Content Automation Protocol (SCAP) and provides vulnerability data feeds for compliance with the SCAP FDCC capable family of tools.
NVD Overview

**Vulnerabilities**
- 72,000+
  - Over 72,000 CVE entries

**Product Names**
- 105,000+
  - Product dictionary containing over 105,000 unique CPE based product names

**Checklists**
- 290+
  - Over 290 Checklists posted.

**New Vulnerabilities**
- 6,000+
  - The NVD Analysis Team evaluates over 6,000 vulnerabilities a year

**SCAP Checklists**
- 80+
  - 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/scappproducts.cfm](http://nvd.nist.gov/scappproducts.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](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

PRIVATE

SEI CERT
- Discovery
- Collection
- Analysis
- Coordination

DHS US-CERT
- Request
- Notification

MITRE CVE
- Reserved CVE Allocation

NIST NVD

OTHERS
- Private Report
- Vendors, Researchers

PUBLIC

Reserved CVE Allocation

Collection

CVE Assignment

NCAS: Vulnerability Notes, Current Activity, Alerts

Catalog

CVSS, SCAP additions

NCAS: Vulnerability Notes, Current Activity, Alerts

Public Disclosure

CNA Assignment

Public Disclosure
National Vulnerability Database Role

Receive CVE Information from MITRE
- ID
- Description
- References

NVD Analysis
- Metrics
- Vulnerability Category
- Product Configuration

Data Feeds
- Public Sector
- Private Sector
- Commercial Vendors
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

Impact
CVSS v2 Score: 9.0 (HIGH) [AV:N/AC:L/Au:NA/C:C/I:C/A:0]
Impact Subscore: 9.0
Exploitability Subscore: 3.7
CVE SS Version 2 Metrics:
Access Vector: Network.
Authentication: Not required.
Impact Type: Provides administrator access, allows complete control of the system. Allows stealing of secrets.

References to Advisories, Solutions, and Tools
By selecting these links, you will be leaving NIST web page. 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/ncas/alerts/TA08-253A

External Source: MISC
Name: http://www.msrc.com/advisory/TEST
Hyperlink: http://www.msrc.com/advisory/TEST

External Source: CIPPS
Name: http://www.cipps.org/advisory/TEST
Hyperlink: http://www.cipps.org/advisory/TEST

External Source: DISA
Name: http://www.disa.mil/ADVISORY/TEST
Hyperlink: http://www.disa.mil/ADVISORY/TEST

External Source: VUPEN
Name: ADV-2008-2520
Type: Advisory

External Source: VUPEN
Name: ADV-2008-2596
Type: Advisory

External Source: VUPEN
Name: ADV-2008-2583
Type: Advisory

Technical Details
Vulnerability Type: (View All)
Resource Management Errors (CVE-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 cve@nist.gov.
NIST is an Agency of the U.S. Department of Commerce
Publication Date: 09/11/2008
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]

Example:

AV:N/AC:L/Au:S/C:N/I:N/A:P
CVSS v2.0 Temporal Metric

<table>
<thead>
<tr>
<th>Exploitability (E)</th>
<th>Remediation Level (RL)</th>
<th>Report Confidence (RC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Unproven (U)</td>
<td>• Official Fix (OF)</td>
<td>• Unconfirmed (UC)</td>
</tr>
<tr>
<td>• Functional (F)</td>
<td>• Temporary Fix (TF)</td>
<td>• Uncorroborated (UR)</td>
</tr>
<tr>
<td>• High (H)</td>
<td>• Workaround (W)</td>
<td>• Confirmed (C)</td>
</tr>
<tr>
<td>• Not Defined (ND)</td>
<td>• Unavailable (U)</td>
<td>• Not Defined (ND)</td>
</tr>
<tr>
<td></td>
<td>• Not Defined (ND)</td>
<td></td>
</tr>
</tbody>
</table>
## CVSS v2.0 Environmental Metrics

<table>
<thead>
<tr>
<th>Collateral Damage Potential (CDP)</th>
<th>Target Distribution (TD)</th>
<th>Security Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (N)</td>
<td>None (N)</td>
<td>Confidentiality Requirement (CR)</td>
</tr>
<tr>
<td>Low (L)</td>
<td>Low (L)</td>
<td>Integrity Requirement (IR)</td>
</tr>
<tr>
<td>Low-Medium (LM)</td>
<td>Medium (M)</td>
<td>Availability Requirement (AR)</td>
</tr>
<tr>
<td>Medium-High (MH)</td>
<td>High (H)</td>
<td>Low (L)</td>
</tr>
<tr>
<td>High (H)</td>
<td>Not Defined (ND)</td>
<td>Medium (M)</td>
</tr>
<tr>
<td>Not Defined (ND)</td>
<td></td>
<td>High (H)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not Defined (ND)</td>
</tr>
</tbody>
</table>
CVSS v3.0 Base Metrics

Exploitability
- Attack Vector (AV)
  - Network (N)
  - Adjacent (A)
  - Local (L)
  - Physical (P)
- Attack Complexity (AC)
  - Low (L)
  - High (H)
- Privileges Required (PR)
  - None (N)
  - Low (L)
  - High (H)
- User Interaction
  - None
  - Required

Scope
- Unchanged (U)
- Changed (C)

Impact
- Confidentiality (C)
  - High (H)
  - Low (L)
  - None (N)
- Integrity (I)
  - High (H)
  - Low (L)
  - None (N)
- Availability (A)
  - High (H)
  - Low (L)
  - None (N)
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]

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

<table>
<thead>
<tr>
<th>Exploit Code Maturity (E)</th>
<th>Remediation Level (RL)</th>
<th>Report Confidence (RC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Not Defined (X)</td>
<td>• Not Defined (X)</td>
<td>• Not Defined (X)</td>
</tr>
<tr>
<td>• High (H)</td>
<td>• Unavailable (U)</td>
<td>• Confirmed (C)</td>
</tr>
<tr>
<td>• Functional (F)</td>
<td>• Workaround (W)</td>
<td>• Reasonable (R)</td>
</tr>
<tr>
<td>• Proof-of-Concept (P)</td>
<td>• Temporary Fix (TF)</td>
<td>• Unknown (U)</td>
</tr>
<tr>
<td>• Unproven (U)</td>
<td>• Official Fix (OF)</td>
<td></td>
</tr>
</tbody>
</table>
### 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](http://nvd.nist.gov)

- **National Checklist Program**
  - [http://checklists.nist.gov](http://checklists.nist.gov)

- **SCAP Homepage**
  - [http://scap.nist.gov](http://scap.nist.gov)

- **SCAP Validated Products**
  - [http://nvd.nist.gov/scapproducts.cfm](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/PubsSPs.html)
  - [http://csrc.nist.gov/publications/PubsNISTIRs.html](http://csrc.nist.gov/publications/PubsNISTIRs.html)