The Current State of Vulnerability Reporting

Harold Booth
Overview

- Global Vulnerability Reporting
- The United States
- Japan
Global Vulnerability Reporting

- Does not currently exist
- Each region has own processes with little or no communication
- Some sharing occurs through public databases (NVD, JVN, Secunia, SecurityFocus, OSVDB, ISS X-Force)
- Often work is duplicated due to language issues
Vulnerability Formats

- Common Announcement Interchange Format (CAIF)
- Common Vulnerability Reporting Format (CVRF)
- Japan Vulnerability Notes (JVN)
- Vulnerability Data Model (Proposed Draft to IETF) – based on the NVD data model
- Proprietary formats
  - Vendor Advisories
  - Vulnerability Databases
- Varying levels of machine processing
Reporting in the US

- Some best practices have been established
  - Responsible disclosure
  - Timely Vendor response
- Voluntary
- Disseminate information as widely as possible
  - Administrators need to know
  - Malicious actors already know
Noteworthy Participants

- CERT/CC – assists in coordinating vulnerability reports as well as produces tools for identifying vulnerabilities in software
- US-CERT – alerts for noteworthy vulnerabilities
- ICS-CERT – assists in coordinating vulnerability reports for industrial control systems
- MITRE – moderates CVE dictionary process
- NIST – maintains the National Vulnerability Database (NVD) and participates in standards development activities (i.e. CVSSv3)
- Vendors – level of participation varies from vendor to vendor
- Security Researchers – Discover and report vulnerabilities
CVE/NVD (US) Ecosystem

SEI CERT
- Discovery
- Collection
- Analysis
- Coordination

DHS US-CERT
- Request
- Notification

MITRE CVE
- Reserved CVE Allocation

NIST NVD

Others
- Private Report
- Vendors, Researchers

Private

Public
- Collection
- Analysis
- CVE Assignment
- Publication

NCAS: Vulnerability Notes, Current Activity, Alerts

Public Disclosure
- CNA Assignment

D/A and private sector vulnerability response, patch management

Catalog
- CVSS, SCAP additions
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
  - Description
  - References
CVE (continued)

- **CVE Numbering Authorities (CNA)**
  - Vendors and other organizations involved in the disclosure process
  - Assigns a CVE identifier to a vulnerability from a pre-allocated set of CVE identifiers

- **CVE are created based upon:**
  - CNAs
  - Vendor submission
  - Discovery based upon monitoring of information sources (Vendors, Security Databases, etc….)
Contains all vulnerabilities published in the CVE dictionary

Provides a base score value according to the Common Vulnerability Scoring System (CVSS) Version 2

Categorizes and verifies references

Relates product applicability using the Common Platform Enumeration (CPE)

Categorizes each vulnerability using Common Weakness Enumeration (CWE)
Vulnerability Summary for CVE-2008-3013

Original release date: 09/11/2008
Last revised: 10/18/2011
Source: US-CERT/NIST

Overview

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) (legend)
Impact Subscore: 10.0
Exploitability Subscore: 8.6

CVSS Version 2 Metrics:
Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type: Provides administrator access, Allows complete confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information; Allows disruption of service
References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webservice. 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/TA08-253A.html](http://www.us-cert.gov/cas/techalerts/TA08-253A.html)

**External Source**: MISC
**Name**: [http://www.zerodayinitiative.com/advisories/ZDI-08-056/](http://www.zerodayinitiative.com/advisories/ZDI-08-056/)

**External Source**: MISC
**Name**: [http://www.zerodayinitiative.com/advisories/ZDI-08-056/](http://www.zerodayinitiative.com/advisories/ZDI-08-056/)

**External Source**: VUPEN
**Name**: ADV-2008-2696
**Type**: Advisory

**External Source**: VUPEN
**Name**: ADV-2008-2520
CVE Detail for NVD – Check Content and Configurations

References to Check Content

Identifier: oval:org.mitre.oval:oval:def:5986
Check System: http://oval.mitre.org/XMLSchema/oval-definitions-5

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:works:8
    - cpe:a:microsoft:forefront_client_security:1.0

* Denotes Vulnerable Software