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

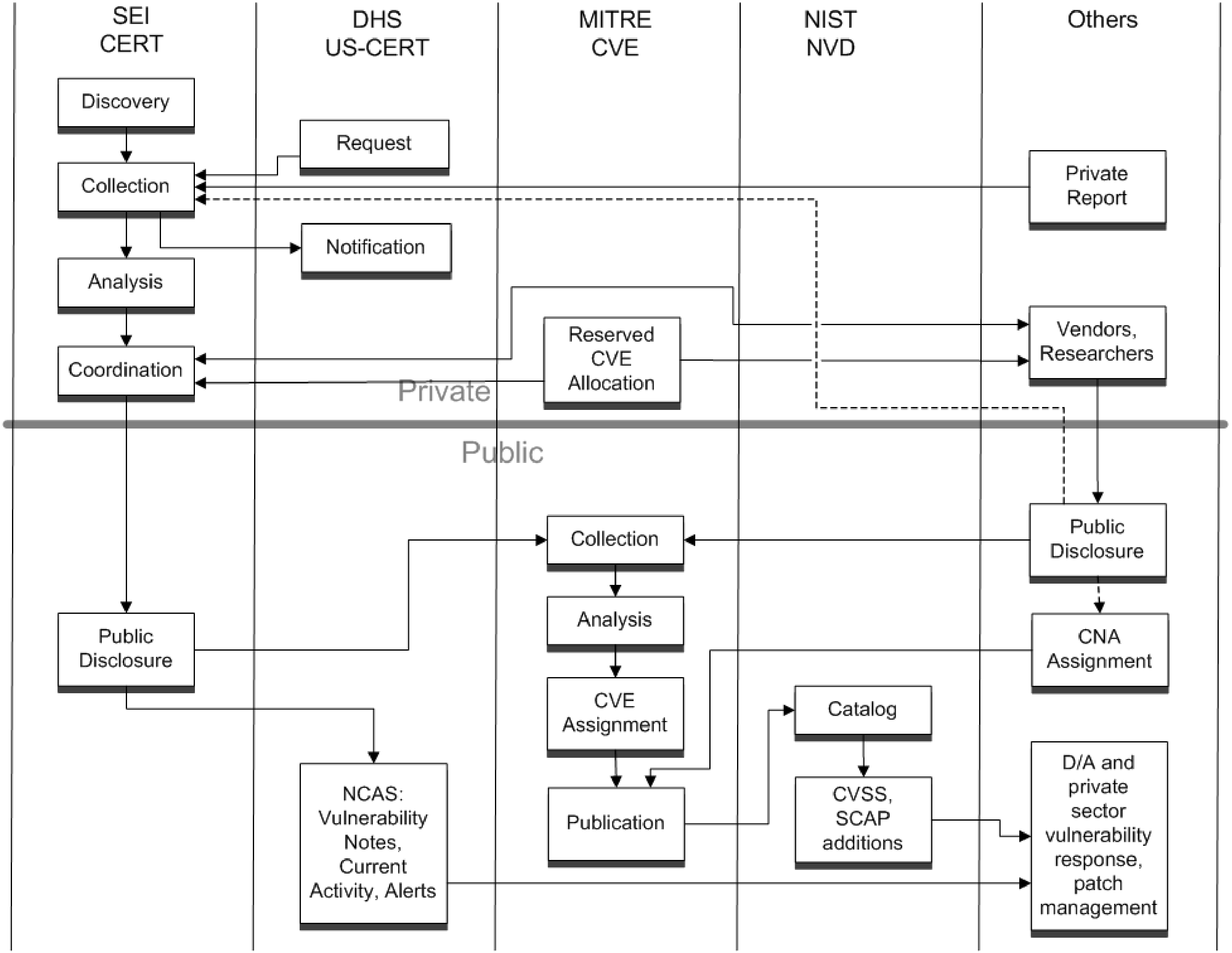
Reporting in the US

- 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



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

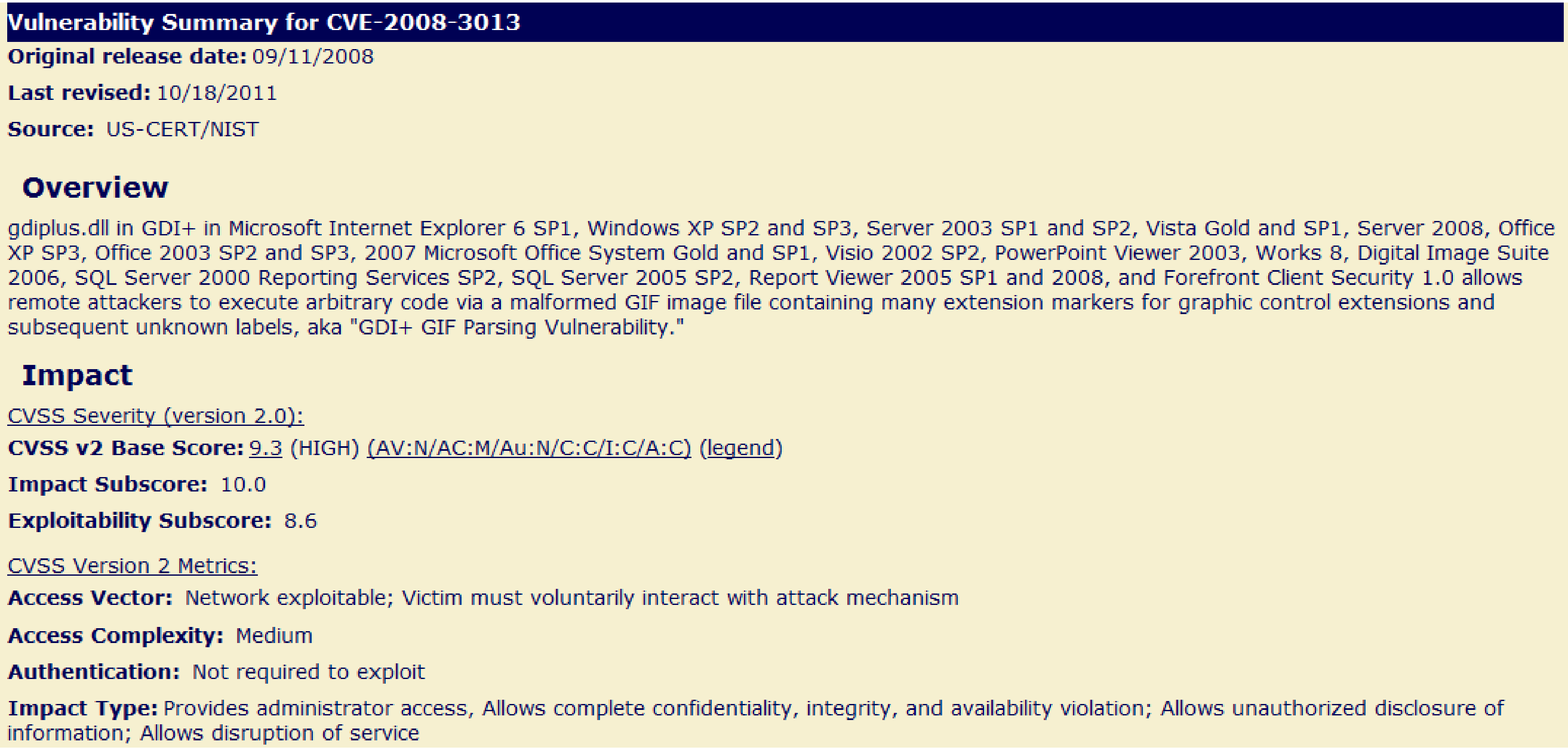
CVE (continued)

- 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…)

National Vulnerability Database (NVD)

- 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)

CVE Detail for NVD – Summary and CVSS Base Score



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 SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, Server 2008, Office XP SP3, Office 2003 SP2 and SP3, 2007 Microsoft Office System Gold and SP1, Visio 2002 SP2, PowerPoint Viewer 2003, Works 8, Digital Image Suite 2006, SQL Server 2000 Reporting Services SP2, SQL Server 2005 SP2, Report Viewer 2005 SP1 and 2008, and Forefront Client Security 1.0 allows remote attackers to execute arbitrary code via a malformed GIF image file containing many extension markers for graphic control extensions and 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) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

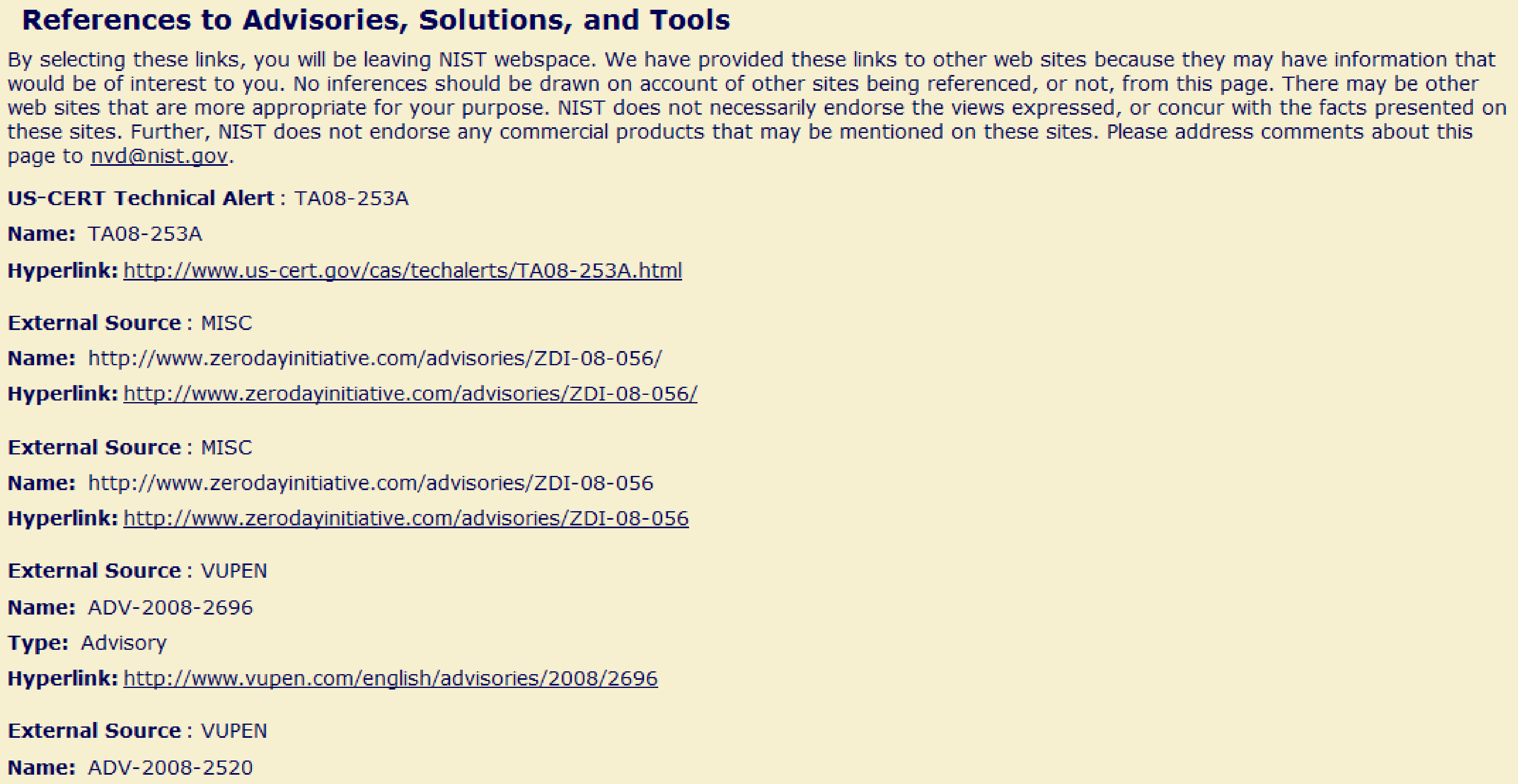
Access Vector: Network exploitable; Victim must voluntarily interact with attack mechanism

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

CVE Detail for NVD - References



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/TA08-253A.html

External Source : MISC

Name: http://www.zerodayinitiative.com/advisories/ZDI-08-056/

Hyperlink: http://www.zerodayinitiative.com/advisories/ZDI-08-056/

External Source : MISC

Name: http://www.zerodayinitiative.com/advisories/ZDI-08-056

Hyperlink: http://www.zerodayinitiative.com/advisories/ZDI-08-056

External Source : VUPEN

Name: ADV-2008-2696

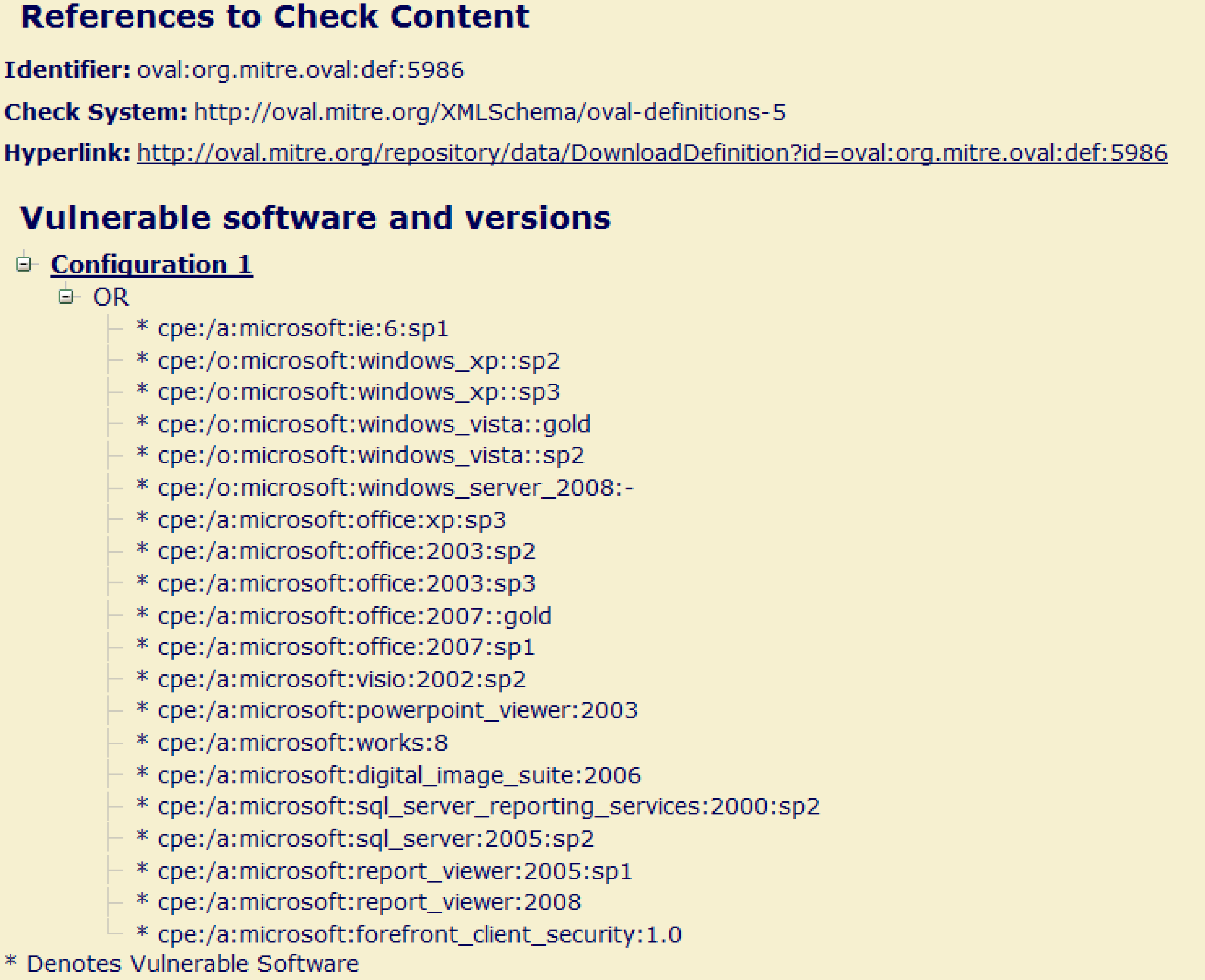
Type: Advisory

Hyperlink: http://www.vupen.com/english/advisories/2008/2696

External Source : VUPEN

Name: ADV-2008-2520

CVE Detail for NVD – Check Content and Configurations



References to Check Content

Identifier: oval:org.mitre.oval:def:5986

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

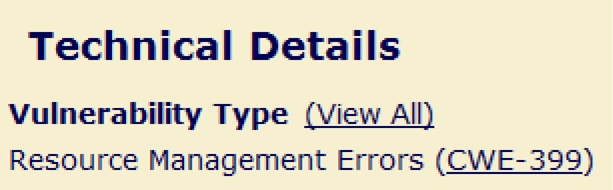
Hyperlink: http://oval.mitre.org/repository/data/DownloadDefinition?id=oval:org.mitre.oval:def:5986

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

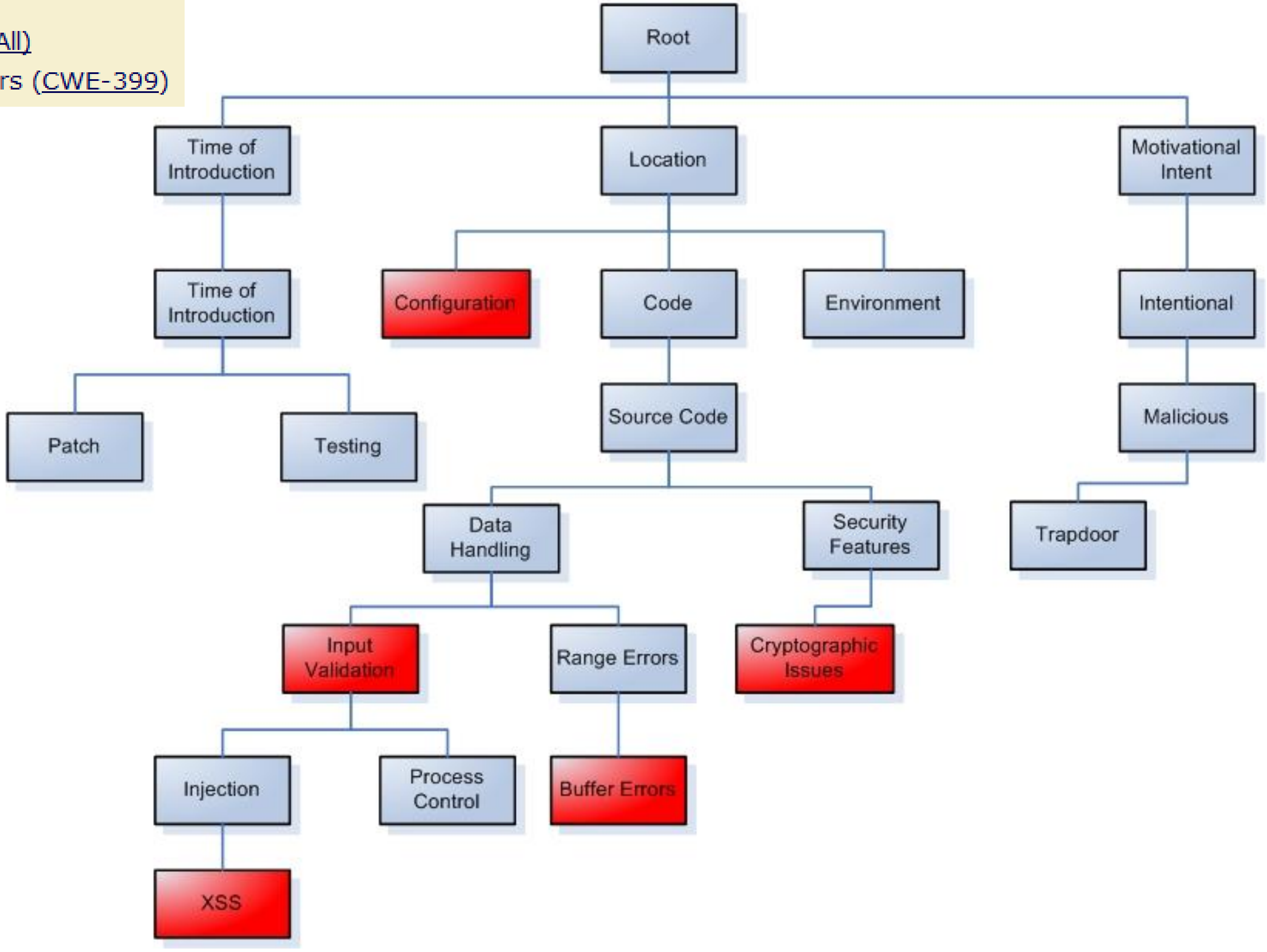
CVE Detail for NVD - CWE



Technical Details

Vulnerability Type (View All)

Resource Management Errors (CWE-399)



Portion of CWE Structure