# CVEdetails.com

Serkan Özkan

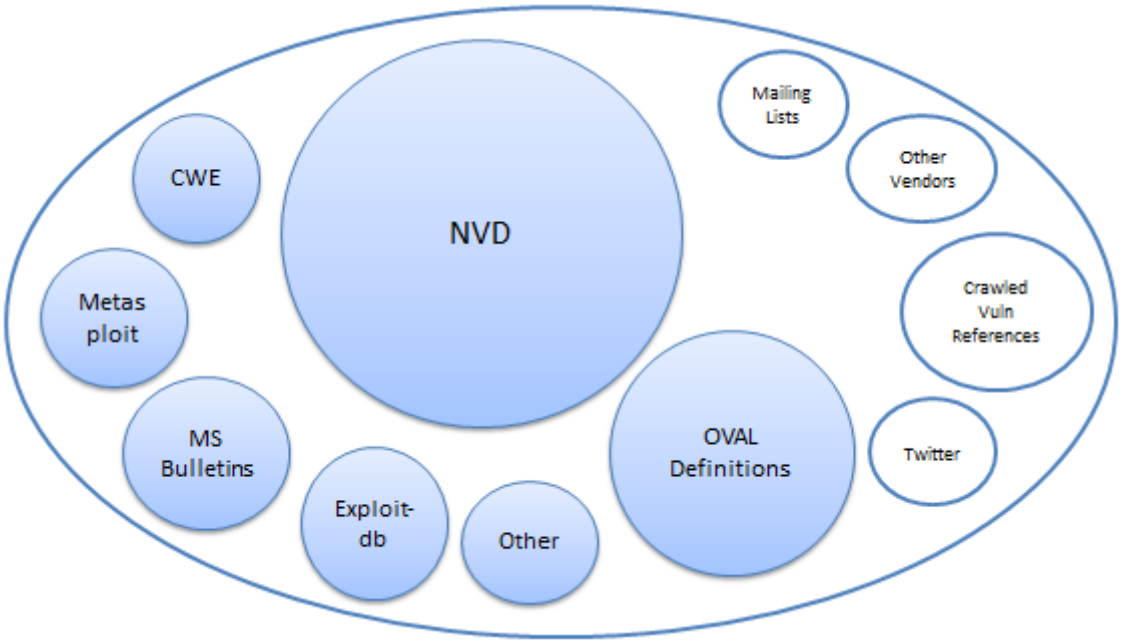
serkanozkan @ gmail.com

# Introduction

- Easy to use interface for vulnerability data
- Data from several sources
- Browsable by vendor, product, version, type, date…
- Vulnerability statistics, trends, reports
- Integrated OVAL definitions

CVEdetails.com is a vulnerability database web site, developed by Serkan Özkan,me , as a personal project. Since I was tired of looking for a reliable and easy to use data source for vulnerabilities I developed CVEdetails.com. When I need a way to view related OVAL definitions I developed itsecdb.com.
Vulnerabilities and other data like vendors, products and versions are all browsable so it is easier to find what you are looking for.
CVEdetails.com provides unique vulnerability statistics and reports.
Data from several sources are merged by CVEdetails.com, which allows users to access information easily.

# Data Sources




Data sources with white backgrounds are not added yet but work is in progress.
NVD is the main data source. OVAL definitions are imported from several sources including Mitre, NIST, Red Hat etc.
Other data includes : Additional vendor supplied data (currently available only for Red Hat products)

# NVD – Main Data Source

- NVD CVE XML feeds
- Updated daily
- XML data => database
- CPE Names => Vendor, product and versions
- The data is as good/bad as NVD data
- Improvements in NVD data quality will automatically improve CVEdetails data

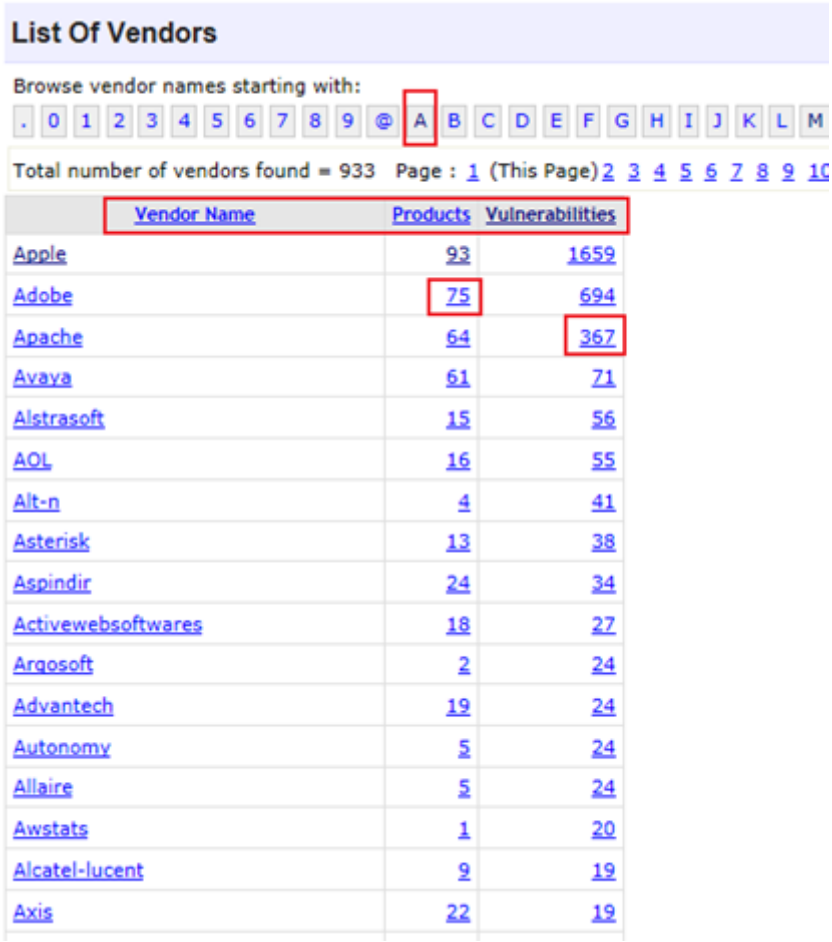
More information about NVD feeds can be found at http://nvd.nist.gov/download.cfm
NVD data quality may be improved. CVEdetails.com already has some features (like ratings, item merge suggestions) that may be used to improve data quality. (but those features are not popular)
Data collected from all sources are processed and correlated using CVE ids and URIs.

# Features

- Browsable : By vendor, product, version, category, date…
- Sortable : By CVSS Scores, number of vulnerabilities …
- Searchable : Vendors, products, versions, vulnerabilities …
- Categorized : Sql injection, XSS, DoS …
- Reporting : Vulnerability statistics, trends for vendors, dates
- Integration : RSS feeds, embeddable widgets, JSON API

Browsable : Vendors, products, versions, vulnerabilities and several other data are easily browsable
Categorized : Vulnerabilities categorized by keyword matching and cwe ids
Sortable : All listings are sortable, by cvss scores, alphabetically, by date etc.
Searchable : Vendor, product, version and vulnerability search
Reportable : CVEdetails.com includes several unique vulnerability reports
Integration : CVEdetails.com provides rss feeds, embedable widgets and json api for integration with other applications, sites

# Browsable, Sortable



List Of Vendors

Browse vendor names starting with:

. 0 1 2 3 4 5 6 7 8 9 @ A B C D E F G H I J K L M

Total number of vendors found = 933 Page : 1 (This Page) 2 3 4 5 6 7 8 9 10

| Vendor Name | Products | Vulnerabilities |
|---|---|---|
| Apple | 93 | 1659 |
| Adobe | 75 | 694 |
| Apache | 64 | 367 |
| Avaya | 61 | 71 |
| Alstrasoft | 15 | 56 |
| AOL | 16 | 55 |
| Alt-n | 4 | 41 |
| Asterisk | 13 | 38 |
| Aspindir | 24 | 34 |
| Activewebsoftwares | 18 | 27 |
| Argosoft | 2 | 24 |
| Advantech | 19 | 24 |
| Autonomy | 5 | 24 |
| Allaire | 5 | 24 |
| Awstats | 1 | 20 |
| Alcatel-lucent | 9 | 19 |
| Axis | 22 | 19 |

List of vendors can be filtered by initial character of vendor name.
The list can be sorted by vendor name, number of products and number of vulnerabilities.

# Browsable, Sortable

## Security Vulnerabilities Published In February 2012

**2012** : January February March CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : Cve Number Descending Cve Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **353** Page : 1 (This Page) 2 3 4 5 6 7 8

| # | CVE ID | CWE ID | # of Exploits | Vulnerability Type(s) | Publish Date | Update Date | Score | Gained Access Level | Access | Complexity | Authentication | Confidentiality | Integrity | Availability |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | CVE-2012-1418 | | | | 2012-02-29 | 2012-02-29 | 10.0 | None | Remote | Low | Not required | Complete | Complete | Complete |
| | Multiple unspecified vulnerabilities in Google Chrome before 17.0.963.60 on the Acer AC700, Samsung Series 5, and Cr-48 Chromebook platforms have unknown impact and attack vectors. | | | | | | | | | | | | | |
| 2 | CVE-2012-1410 | 79 | | XSS | 2012-02-29 | 2012-02-29 | 4.3 | None | Remote | Medium | Not required | None | Partial | None |
| | Multiple cross-site scripting (XSS) vulnerabilities in the History Window implementation in Kadu 0.9.0 through 0.11.0 allow remote attackers to inject arbitrary web script or HTML via a crafted (1) SMS message, (2) presence message, or (3) status description. | | | | | | | | | | | | | |
| 3 | CVE-2012-1294 | 89 | 1 | Exec Code Sql | 2012-02-23 | 2012-02-24 | 7.5 | None | Remote | Low | Not required | Partial | Partial | Partial |
| | SQL injection vulnerability in CONTIMEX Impulsio CMS allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php. | | | | | | | | | | | | | |
| 4 | CVE-2012-1292 | | | +Info | 2012-02-23 | 2012-02-27 | 5.0 | None | Remote | Low | Not required | Partial | None | None |
| | Unspecified vulnerability in the MessagingSystem servlet in SAP NetWeaver 7.0 allows remote attackers to obtain sensitive information about the MessagingSystem Performance Data via unspecified vectors. | | | | | | | | | | | | | |

List of vulnerabilities can be filtered by year, month, cvss scores. The list can be sorted by cve ids, cvss scores and number of exploits.

# Categorized

## Apple : Vulnerability Statistics

Products (93) Vulnerabilities (1659) Search for products of Apple CVSS Scores Report Possible matches for this vendor Related Metasploit Modules

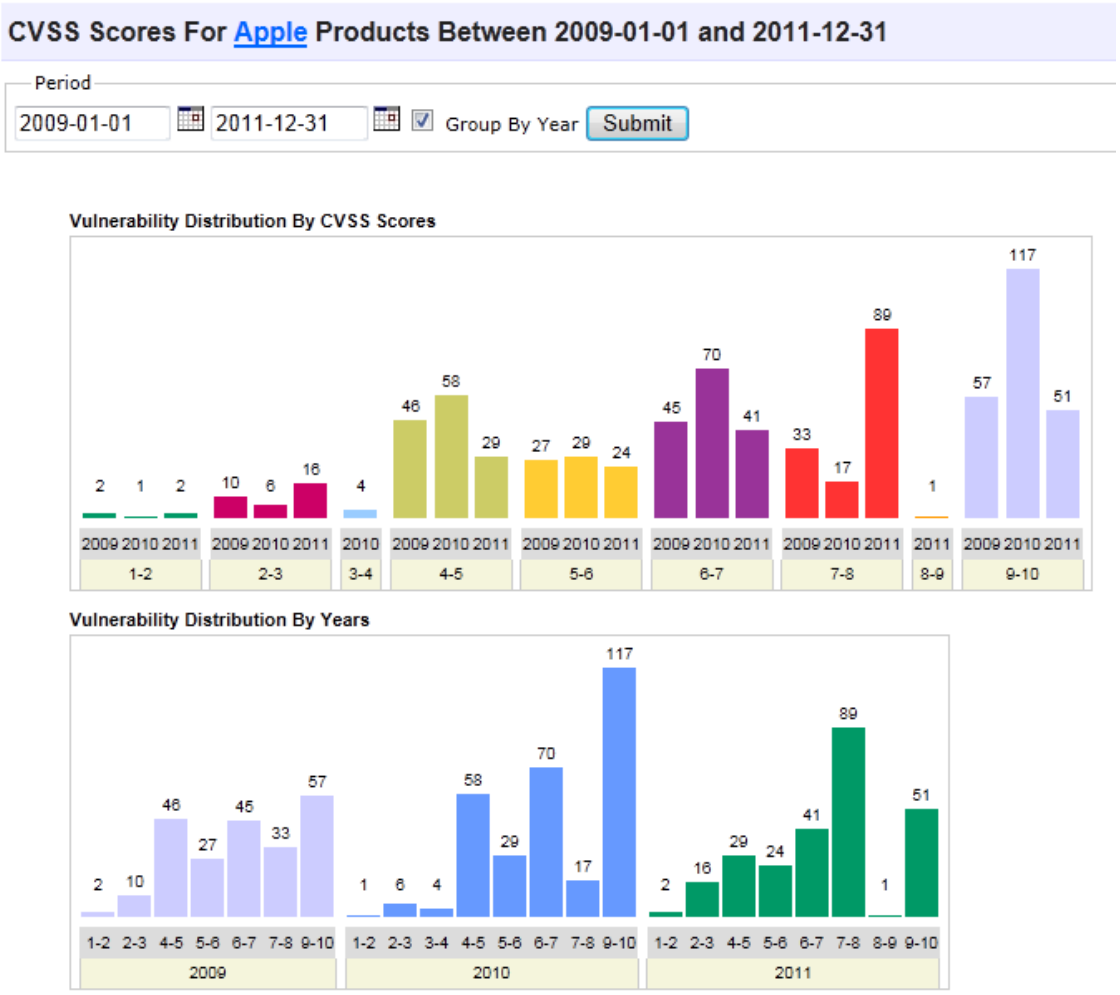
Vulnerability Feeds & Widgets New

### Vulnerability Trends Over Time

| Year | # of Vulnerabilities | DoS | Code Execution | Overflow | Memory Corruption | Sql Injection | XSS | Directory Traversal | Http Response Splitting | Bypass something | Gain Information | Gain Privileges | CSRF | File Inclusion | # of exploits |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1999 | 7 | 1 | | | | | | | | 3 | | | | | |
| 2000 | 4 | 1 | | 1 | | | | | | | | | | | |
| 2001 | 12 | 3 | 3 | 3 | | | | | | | 1 | 2 | | | |
| 2002 | 23 | 7 | 10 | 5 | | | | | | | | 2 | | | 1 |
| 2003 | 47 | 7 | 10 | 9 | | | 1 | 3 | | | 1 | 4 | | | |
| 2004 | 66 | 8 | 13 | 10 | | | | 2 | | 3 | 2 | 5 | | | |
| 2005 | 148 | 28 | 45 | 38 | 1 | | 2 | 1 | | 7 | 4 | 12 | | | |
| 2006 | 138 | 42 | 72 | 53 | 5 | | 1 | 1 | | 6 | 5 | 6 | | | |
| 2007 | 208 | 62 | 99 | 58 | 20 | | 13 | 2 | 1 | 19 | 13 | 18 | | | 6 |
| 2008 | 211 | 76 | 102 | 54 | 21 | | 12 | 3 | | 15 | 29 | 7 | 1 | | 10 |
| 2009 | 220 | 108 | 96 | 61 | 24 | | 17 | | 1 | 12 | 23 | 9 | 1 | | 16 |
| 2010 | 302 | 174 | 165 | 84 | 40 | | 12 | 5 | | 22 | 27 | 10 | 1 | | 8 |
| 2011 | 253 | 169 | 169 | 149 | 108 | | 9 | 2 | | 15 | 23 | 3 | | | 1 |
| 2012 | 15 | 10 | 10 | 5 | 3 | | | | | | 3 | 1 | | | |
| Total | 1654 | 696 | 794 | 530 | 222 | | 67 | 19 | 2 | 102 | 131 | 79 | 3 | | 42 |
| % Of All | | 42.1 | 48.0 | 32.0 | 13.4 | 0.0 | 4.1 | 1.1 | 0.1 | 6.2 | 7.9 | 4.8 | 0.2 | 0.0 | |

Vulnerabilities are categorized by keyword matching and cwe ids. Categorization provides easier access to vulnerabilities.

# Reports



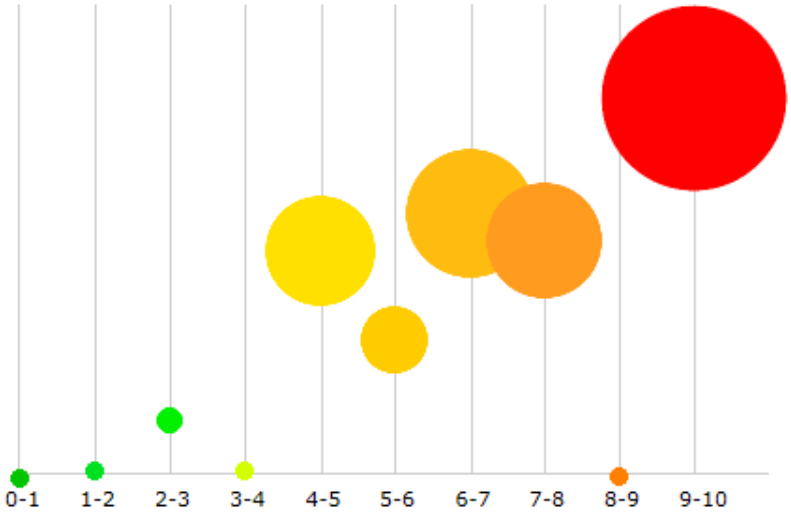

It is possible to generate a cvss score report for vendors, products or versions.
In this screenshot vulnerability score distributions are compared for 2009,2010 and 2011

# Reports

## CVSS Scores For Apple Products Between 2009-01-01 and 2011-12-31

Period

2009-01-01 2011-12-31 Group By Year Submit




This chart shows distribution of cvss scores of vulnerabilities of Apple products between 2009 and 2012. Bubble sizes represent number of vulnerabilities in the given range.

# Integration

- RSS Feeds
- Embedable widgets
- JSON API
- All integration options are customizable by :
    - Vulnerability types
    - CVSS scores
    - Exploits
    - Vendors, products and versions

Customizable feeds allows users to subscribe for feeds that fit their needs. For example a user can subscribe for vulnerabilities of all Oracle products, or vulnerabilities of any version of Microsoft Sql Server, or vulnerabilities of PHP 5.3.2. Or a user can subscribe for only sql injection and cross site scripting vulnerabilities of Wordpress.
Vulnerability list widgets can be embedded into any web page as an iframe.

# Custom Feeds & Widgets


Custom feed and widget generation for Apple Mac Os X.
It is possible to generate custom widgets or feeds for any vendor, product or version.
For example you can subscribe for only sql injection vulnerabilities of a specific version of Joomla.

# Embedable Widget

CVE-2011-3463 CVSS:7.2

WebDAV Sharing in Apple Mac OS X 10.7.x before 10.7.3 does not properly perform authentication, which allows local users to gain privileges by leveraging access to (1) the server or (2) a bound directory. *(Last Update:2012-02-03) (Publish Update:2012-02-02)*

CVE-2011-3462 CVSS:5.0

Time Machine in Apple Mac OS X before 10.7.3 does not verify the unique identifier of its remote AFP volume or Time Capsule, which allows remote attackers to obtain sensitive information contained in new backups by spoofing this storage object, a different vulnerability than CVE-2010-1803. *(Last Update:2012-02-03) (Publish Update:2012-02-02)*

CVE-2011-3460 CVSS:7.5

Buffer overflow in QuickTime in Apple Mac OS X before 10.7.3 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PNG file. *(Last Update:2012-02-03) (Publish Update:2012-02-02)*

CVE-2011-3459 CVSS:6.8

Off-by-one error in QuickTime in Apple Mac OS X before 10.7.3 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted rdrf atom in a movie file that triggers a buffer overflow. *(Last Update:2012-02-03) (Publish Update:2012-02-02)*

CVE-2011-3458 CVSS:6.8

QuickTime in Apple Mac OS X before 10.7.3 does not prevent access to uninitialized memory locations, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted MP4 file. *(Last Update:2012-02-03) (Publish Update:2012-02-02)*

# Vulnerability Details

- Vulnerability details
- CVSS score
- Related OVAL definitions
- Products & versions affected by the vulnerability
- References (with some additional details)
- Related metasploit modules
- Quick links to external sources
- User comments
- Additional vendor data (if available)

External sources include Secunia, Nessus plugins, NVD, Mitre, Xforce
Registered users of CVEdetails.com can add comments to CVE entries.
Additional vendor data is only available for Red Hat products (since only Red Hat provides such data)

# Vulnerability Details

## Vulnerability Details : CVE-2011-0654 (1 public exploit)

Integer underflow in the BowserWriteErrorLogEntry function in the Common Internet File System (CIFS) browser service in Mrxsmb.sys or bowser.sys in Active Directory in Microsoft Windows XP SP2 and SP3, Windows Server 2003 SP2, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, R2, and R2 SP1, and Windows 7 Gold and SP1 allows remote attackers to execute arbitrary code or cause a denial of service (system crash) via a malformed BROWSER ELECTION message, leading to a heap-based buffer overflow, aka "Browser Pool Corruption Vulnerability." NOTE: some of these details are obtained from third party information.

Publish Date : 2011-02-15 Last Update Date : 2011-10-25



### – CVSS Scores & Vulnerability Types

| | |
|---|---|
| Cvss Score | 10.0 |
| Confidentiality Impact | Complete (There is total information disclosure, resulting in all system files being revealed.) |
| Integrity Impact | Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.) |
| Availability Impact | Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.) |
| Access Complexity | Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. ) |
| Authentication | Not required (Authentication is not required to exploit the vulnerability.) |
| Gained Access | None |
| Vulnerability Type(s) | Denial Of Service Execute Code Overflow |
| CWE ID | 119 |

## – Related OVAL Definitions

| Title | Definition Id | Class | Family |
|---|---|---|---|
| Browser Pool Corruption Vulnerability | oval:org.mitre.oval:def:12637 | | windows |
| MS11-019: Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455) | oval:gov.nist.fdcc.patch:def:11742 | | windows |

OVAL (Open Vulnerability and Assessment Language) definitions define exactly what should be done to verify a vulnerability or a missing patch. Check out the OVAL definitions if you want to learn what you should do to verify a vulnerability.

## – Products Affected By CVE-2011-0654

| # | Product Type | Vendor | Product | Version | Update | Edition | Language | |
|---|---|---|---|---|---|---|---|---|
| 1 | OS | Microsoft | Windows 2003 Server | | R2 | | | Details Vulnerabilities |
| 2 | OS | Microsoft | Windows 2003 Server | | | | | Details Vulnerabilities |
| 3 | OS | Microsoft | Windows 2003 Server | | R2 | X64 | | Details Vulnerabilities |
| 4 | OS | Microsoft | Windows 2003 Server | | SP2 | Itanium | | Details Vulnerabilities |
| 5 | OS | Microsoft | Windows Server 2003 | | SP2 | X64 | | Details Vulnerabilities |
| 6 | OS | Microsoft | Windows Server 2003 | | | X64 | | Details Vulnerabilities |
| 7 | OS | Microsoft | Windows Server 2003 | | SP2 | | | Details Vulnerabilities |
| 8 | OS | Microsoft | Windows Server 2003 | | SP2 | Itanium | | Details Vulnerabilities |

## – Number Of Affected Versions By Product

| Vendor | Product | Vulnerable Versions |
|---|---|---|
| Microsoft | Windows 2003 Server | 4 |
| Microsoft | Windows Server 2003 | 4 |

## – References For CVE-2011-0654

http://archives.neohapsis.com/archives/fulldisclosure/current/0284.html
FULLDISC 20110214 MS Windows Server 2003 AD Pre-Auth BROWSER ELECTION Remote Heap Overflow

http://blogs.technet.com/b/mmpc/archive/2011/02/16/my-sweet-valentine-the-cifs-browser-protocol-heap-corruption-vulnerability.aspx CONFIRM

http://secunia.com/advisories/43299
SECUNIA 43299

http://blogs.technet.com/b/srd/archive/2011/02/16/notes-on-exploitability-of-the-recent-windows-browser-protocol-issue.aspx
CONFIRM

http://www.securityfocus.com/bid/46360
BID 46360

**Exploit!** http://www.exploit-db.com/exploits/16166
EXPLOIT-DB 16166 MS Windows Server 2003 AD Pre-Auth BROWSER ELECTION Remote Heap Overflow *Author:*Cupidon-3005 *Release Date:*2011-02-14 (windows) dos

http://www.securitytracker.com/id?1025328
SECTRACK 1025328

http://www.vupen.com/english/advisories/2011/0394
VUPEN ADV-2011-0394

http://www.vupen.com/english/advisories/2011/0938
VUPEN ADV-2011-0938

http://www.us-cert.gov/cas/techalerts/TA11-102A.html
CERT TA11-102A

http://www.microsoft.com/technet/security/bulletin/ms11-019.mspx
Microsoft Security Bulletin MS11-019 MS11-019 - Critical : Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455) - Version: 1.1

http://www.kb.cert.org/vuls/id/323172
CERT-VN VU#323172

http://xforce.iss.net/xforce/xfdb/65376
XF ms-win-server-browser-bo(65376)

## – Metasploit Modules Related To CVE-2011-0654

### Microsoft Windows Browser Pool DoS

This module exploits a denial of service flaw in the Microsoft Windows SMB service on versions of Windows Server 2003 that have been configured as a domain controller. By sending a specially crafted election request, an attacker can cause a pool overflow. The vulnerability appears to be due to an error handling a length value while calculating the amount of memory to copy to a buffer. When there are zero bytes left in the buffer, the length value is improperly decremented and an integer underflow occurs. The resulting value is used in several calculations and is then passed as the length value to an inline memcpy operation. Unfortunately, the length value appears to be fixed at -2 (0xfffffffe) and causes considerable damage to kernel heap memory. While theoretically possible, it does not appear to be trivial to turn this vulnerability into remote (or even local) code execution.

---

Detailed list of affected products and versions; and list of related references.
Some references include additional data not provided by NVD like exploit information from exploit-db
Metasploit modules (if any) related to the CVE entry are also listed in vulnerability details page.

# OVAL Integration – www.itsecdb.com

- www.itsecdb.com, is another project by Serkan Özkan
- OVAL definitions from several sources like Mitre, Red Hat, NIST etc
- Easy to use, human readable interface for OVAL data
- Full OVAL definition details with variable expansion

Full OVAL definitions with variable expansion is a unique feature of itsecdb.com and allows users to view exactly what is defined by the OVAL definition.
OVAL definitions may contain variable references which should be evaluated at runtime. For example if a variable contains the value read from a registry key this value can be referenced in another OVAL definition. itsecdb.com resolves these references and expands referenced variable values.

# Advantages

- Saves a lot of time, saves you from getting lost in OVAL xml jungle
- Allows you to manually verify vulnerabilities exactly the same way as automated scanners
- Fully integrated, cross referenced with CVEdetails
- Browsable by source, type, vendor, product, versions
- Browsable by specific objects (file, registry keys etc)

OVAL xmls are really complex files with several cross references and it is really hard to manually view full details of an OVAL definition.
If you want to manually and precisely verify an OVAL definition you need to read first.
All OVAL data is cross referenced with CVE data so users can navigate between OVAL definitions, CVEs, vendors, products and versions.
Browsing by OVAL objects is a great feature of itsecdb.com, which allow users to view a list of all definitions related to a specific object like a file, a registry key etc.

# Readable OVAL Definition

**The system is vulnerable**

- IF : All of the following are true Software section
  - IF : Windows Server 2003 is installed
    - Windows : Registry Test : Windows Server 2003 is installed

      At least one of the objects listed below must exist on the system (Existence check)

      Windows : Registry Object This registry key holds the version of the installed operating system.
      **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion : CurrentVersion**

      **value** (equals) **5.2**

      The registry key has a value of 5.2 windows : registry_state
  - IF : the version of msasn1.dll is less than 5.2.3790.139
    - Windows : File Test : the version of msasn1.dll is less than 5.2.3790.139

      At least one of the objects listed below must exist on the system (Existence check)

      Windows : File
      **[[value of ${{windows:registry_object:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion : SystemRoot}}]]\System32\msasn1.dll**

      **version** less than **5.2.3790.139** (datatype=version)

      windows : file_state
  - IF : **NOT** the patch kb835732 is installed
    - Windows : Registry Test : the patch kb835732 is installed

      At least one of the objects listed below must exist on the system (Existence check)

      Windows : Registry Object
      **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Hotfix\KB835732 : Installed**

      **value** (equals) **1** (datatype=int)

      windows : registry_state

Variable expansion is marked with a yellow background. The value of SystemRoot value under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion key will be read at runtime and placed here. For example if the value of that registry value is C:\Windows then the full path of the file will be C:\Windows\System32\msasn1.dll

# Browsing By Filename

## OVAL Definitions - windows file filename schannel.dll

| Title | Definition Id | Class | Family |
|---|---|---|---|
| MS07-031: Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840) | oval:gov.nist.fdcc.patch:def:431 | Patch | windows |
| MS09-007: Vulnerability in SChannel could allow spoofing (960225) | oval:gov.nist.fdcc.patch:def:11548 | Patch | windows |
| MS10-049: Vulnerabilities in SChannel could allow Remote Code Execution (980436) | oval:gov.nist.USGCB.patch:def:11682 | Patch | windows |
| MS10-049: Vulnerabilities in SChannel could allow Remote Code Execution (980436) | oval:gov.nist.fdcc.patch:def:11682 | Patch | windows |
| MS10-085: Vulnerability in SChannel Could Allow Denial of Service (2207566) | oval:gov.nist.fdcc.patch:def:11712 | Patch | windows |
| SChannel Malformed Certificate Request Remote Code Execution Vulnerability | oval:org.mitre.oval:def:11787 | Vulnerability | windows |
| SChannel Spoofing Vulnerability | oval:org.mitre.oval:def:6011 | Vulnerability | windows |
| SSL and TLS Protocols Vulnerability | oval:org.mitre.oval:def:14752 | Vulnerability | windows |
| TLS/SSL Renegotiation Vulnerability | oval:org.mitre.oval:def:7315 | Vulnerability | windows |
| TLSv1 Denial of Service Vulnerability | oval:org.mitre.oval:def:6806 | Vulnerability | windows |
| Windows 2000 SSL PCT Handshake Vulnerability | oval:org.mitre.oval:def:951 | Vulnerability | windows |
| Windows 2000 SSL Library Denial of Service | oval:org.mitre.oval:def:892 | Vulnerability | windows |
| Windows NT SSL PCT Handshake Vulnerability | oval:org.mitre.oval:def:903 | Vulnerability | windows |
| Windows Security Channel Remote Execution Vulnerability | oval:org.mitre.oval:def:1895 | Vulnerability | windows |
| Windows Server 2003 SSL PCT Handshake Vulnerability | oval:org.mitre.oval:def:1093 | Vulnerability | windows |
| Windows Server 2003 SSL Library Denial of Service | oval:org.mitre.oval:def:885 | Vulnerability | windows |
| Windows XP SSL PCT Handshake Vulnerability | oval:org.mitre.oval:def:889 | Vulnerability | windows |
| Windows XP SSL Library Denial of Service | oval:org.mitre.oval:def:886 | Vulnerability | windows |

Browsing definitions by windows file object : OVAL definitions that refer to schannel.dll
This listing contains OVAL definitions from multiple sources, so a user can easily view OVAL definitions related to schannel.dll

# Browsing By Registry Key

## OVAL Definitions - windows registry key SOFTWARE\Apple Computer, Inc.\Safari

| Title | Definition Id | Class | Family |
|---|---|---|---|
| Apple Safari BMP Image Uninitialized Memory Information Disclosure Vulnerability | oval:org.mitre.oval:def:6885 | Vulnerability | windows |
| Apple Safari Cross-site scripting (XSS) vulnerability. | oval:org.mitre.oval:def:6208 | Vulnerability | windows |
| Apple Safari Denial of Service Vulnerability | oval:org.mitre.oval:def:5559 | Vulnerability | windows |
| Apple Safari ImageIO TIFF Image Remote Code Execution Vulnerability | oval:org.mitre.oval:def:6901 | Vulnerability | windows |
| Apple Safari is installed | oval:org.mitre.oval:def:6325 | Inventory | windows |
| Apple Safari Local HTML Files Information Disclosure Vulnerability. | oval:org.mitre.oval:def:5915 | Vulnerability | windows |
| Apple Safari Malformed URI Remote Denail of Service Vulnerability | oval:org.mitre.oval:def:6091 | Vulnerability | windows |
| Apple Safari Malformed URI Remote Denail of Service Vulnerability | oval:org.mitre.oval:def:6066 | Vulnerability | windows |
| Apple Safari PDF Handling Vulnerability | oval:org.mitre.oval:def:7199 | Vulnerability | windows |
| Apple Safari Prior to 4.0.5 Integer Overflow Vulnerability | oval:org.mitre.oval:def:6741 | Vulnerability | windows |
| Apple Safari Prior to 4.0.5 Configuration Bypass Weakness | oval:org.mitre.oval:def:7051 | Vulnerability | windows |
| Apple Safari Search Path Arbitrary Code Execution Vulnerability | oval:org.mitre.oval:def:11956 | Vulnerability | windows |
| Apple Safari TIFF Image Uninitialized Memory Information Disclosure Vulnerability | oval:org.mitre.oval:def:7561 | Vulnerability | windows |
| Apple Safari URL Obfuscation Vulnerability | oval:org.mitre.oval:def:6812 | Vulnerability | windows |
| Apple Safari URL Schemes Handling Remote Code Execution Vulnerability | oval:org.mitre.oval:def:6817 | Vulnerability | windows |
| Apple Safari WebKit Numeric Character References Remote Memory Corruption Vulnerability. | oval:org.mitre.oval:def:5777 | Vulnerability | windows |

List of OVAL definitions that reference "SOFTWARE\Apple Computer, Inc.\Safari"

# Browsing By Patches - Patch <=> CVE

## OVAL Definitions - hpux patch patch_name PHNE_24395

| Title | Definition Id | Class | Family |
|---|---|---|---|
| HP-UX ftpd Remote Unauthorized Data Access (B.11.04) | oval:org.mitre.oval:def:1029 | Vulnerability | unix |
| HP-UX ftpd Remote Unauthorized Data Access (B.10.24) | oval:org.mitre.oval:def:1212 | Vulnerability | unix |

## Vulnerability oval:org.mitre.oval:def:1029

### HP-UX ftpd Remote Unauthorized Data Access (B.11.04)

Dependent (Extending) Definitions  View Definition At Mitre

The FTP server in HP-UX 10.20, B.11.00, and B.11.11, allows remote attackers to list arbitrary directories as roo command before logging in.

Create Date: 2005-11-30 Last Update Date: 2010-09-20

### Affected Platforms/Products

**Affected Products (CPE + CVE references)**

- HP Hp-ux

**Platforms: unix (from OVAL definitions)**

- HP-UX 11

**Products: unix**

- ftpd

### References

- CVE-2005-3296

Users can view list of OVAL definitions related to a patch, and the OVAL definition is linked to a CVE entry. So it is possible to see the vulnerabilities fixed by this patch.

# Planned Features

- Vulnerability data from more sources : twitter, mailing lists, other vendors, by crawling reference urls
- Vulnerability alerts by email*
- More SCAP implementation, starting with OCIL (Open Checklist Interactive Language)

* If a sponsor is found
I've already completed most of the required work to add data from mailing lists, twitter and crawling vulnerability references.
Vulnerability alerts need a decent hosting solution which requires a sponsor or more resources.
I believe OCIL checklists can be useful and I am planning to add OCIL checklists to CVEdetails.com in the near future. (Users will be able to complete and evaluate questionnaires online)

# Even More

- Working on a (authenticated) vulnerability scanner/analyzer which will use both structured (OVAL, CVE data etc) and non-structured data (definitions, references, mostly free text) to discover vulnerabilities

This project is progressing really very slowly, since I don’t have enough time to work on it.