WARNING & DISCLAIMER

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and CyberSecurity Malaysia shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Vulnerability Name	1. Microsoft Word Unspecified Code Execution Vulnerability
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	9 July 2008
Classification	Remote Code Execution
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2244
Affected Products	Microsoft Word 2002 SP3
Description	A vulnerability was reported in Microsoft Word. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can create a specially crafted document that, when loaded by the target user, will trigger a memory corruption error and execute arbitrary code on the target system. The code will run with the privileges of the target user. The vulnerability is reported in Microsoft Word 2002 SP3 and is currently not believed to affect other versions.
Impact	System access from remote. A remote user can create a file that, when loaded by the target user, will execute arbitrary code on the target user's system.

Solution	The vendor suggests viewing Word documents in Microsoft Office Word 2003 Viewer or Microsoft Office Word 2003 Viewer SP3. Solution Status: Unpatched
References	http://www.microsoft.com/technet/security/advisory/953635.mspx CVE Reference: CVE-2008-2244 http://secunia.com/advisories/30975/

Vulnerability Name	2. Microsoft Access Snapshot Viewer ActiveX Control Vulnerability
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	7 July 2008
Classification	Malicious input
Severity Rating	Medium http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2463
Affected Products	Microsoft Access 2000 Microsoft Access 2002 Microsoft Access 2003 Microsoft Access Snapshot Viewer Microsoft Office 2000 Microsoft Office 2003 Professional Edition Microsoft Office 2003 Small Business Edition Microsoft Office 2003 Standard Edition Microsoft Office 2003 Student and Teacher Edition Microsoft Office XP
Description	The Microsoft Office Snapshot Viewer ActiveX control in snapview.ocx, as distributed in the standalone Snapshot Viewer and Microsoft Office Access 2000 through 2003, allows remote attackers to download arbitrary files to a client machine via a crafted HTML document or e-mail message. NOTE: this can be leveraged for code execution by writing to a Startup folder.
Impact	System access from remote
Solution	The vendor recommends some workarounds available at the following URL: http://www.microsoft.com/technet/security/advisory/955179.mspx Although these workarounds will not correct the underlying vulnerability, they help block known attack vectors.

	Solution Status: Unpatched
References	http://www.kb.cert.org/vuls/id/837785 CVE Reference: CVE-2008-2463 http://secunia.com/advisories/30883/

Vulnerability Name	3. Red Hat Certificate System CSR Extension Handling Bug May Let Users Bypass Security Policy
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	3 July 2008
Classification	Security bypass
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1676
Affected Products	Red Hat Certificate System 7.x
Description	The security issue is caused due to an error in the handling of Extensions in certificate signing requests (CSR) where all requested Extensions are added to the issued certificate. This can be exploited to bypass certain security policies, e.g. submit a CSR for a subordinate CA certificate although prohibited in the CA configuration. This may simplify man-in-the-middle attacks against users that trust Certificate Authorities managed by Red Hat Certificate System.
Impact	Security Bypass from remote.
Solution	The vendor has issued a fix for rhpki-common. Please see the following vendor's advisory for more details: http://rhn.redhat.com/errata/RHSA-2008-0500.html Solution Status: Vendor patch available
References	http://securitytracker.com/alerts/2008/Jul/1020427.html CVE Reference: CVE-2008-1676 http://secunia.com/advisories/30929/

Vulnerability Name	4. Novell eDirectory LDAP Search Request Buffer Overflow
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	11 July 2008
Classification	Buffer Overflow
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1809
Affected Products	Novell eDirectory versions 8.8 and 8.7.3
Description	The vulnerability is caused due to an error in calculating the size of a heap buffer for storing LDAP search parameters. This can be exploited to cause a heap-based buffer overflow with the string "(null)" via NULL search parameters. A remote user can send a specially crafted NULL search parameter to trigger a buffer overflow and execute arbitrary code on the target system. The code will run with the privileges of the target service.
Impact	Denial of Service, system access from local network
Solution	The vendor has issued a fix (8.8.2 FTF2, 8.7.3.10b), available at: http://download.novell.com Solution Status: Vendor patch available
References	https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=178937 www.novell.com/support/viewContent.do?externalId=3843876

	CVE Reference: CVE-2008-1809 http://securitytracker.com/alerts/2008/Jul/1020470.html http://secunia.com/advisories/31036/ http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=724

Vulnerability Name	5. VLC Media Player WAV Processing Integer Overflow
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	2 July 2008
Classification	Remote code execution
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2430
Affected Products	VLC Media Player 0.86h and possibly earlier versions.
Description	A remote user can create a specially crafted WAV file that, when loaded by the target user will trigger an integer overflow and execute arbitrary code on the target system. The code will run with the privileges of the target user. The vulnerability resides in the Open() function in 'modules/demux/wav.c'. Successful exploitation may allow execution of arbitrary code.
Impact	System access from remote
Solution	Do not open untrusted WAV files. The vendor has issued a fixed version (0.8.6i), available at: http://www.videolan.org/vlc/ Solution Status: Fixed version available
References	http://secunia.com/advisories/30601/ CVE Reference: CVE-2008-2430

	http://www.videolan.org/developers/vlc/NEWS http://securitytracker.com/alerts/2008/Jul/1020429.html

Vulnerability Name	6. Microsoft Windows Explorer Saved Search Vulnerability
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	8 July 2008
Classification	Remote code execution
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1435
Affected Products	Microsoft Windows Server 2008 Microsoft Windows Vista
Description	A vulnerability has been reported in Microsoft Windows, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an error in Windows Explorer during the parsing of saved-search (.search-ms) files when saving them. This can be exploited to execute arbitrary code by tricking a user into opening and saving a specially crafted saved-search file.
Impact	System access from remote
Solution	The vendor has issued the following fixes: Windows Vista and Windows Vista Service Pack 1: http://www.microsoft.com/downloads/details.aspx?familyid=06739ca6-7368-4ac b-bb67-7e8146071a29 Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1: http://www.microsoft.com/downloads/details.aspx?familyid=74ea0893-7c2f-4 fad-ad27-588ad953b046

	Windows Server 2008 for 32-bit Systems*: http://www.microsoft.com/downloads/details.aspx?familyid=189a4170-b495-4904-9cbd-209e7494d303 Windows Server 2008 for x64-based Systems*: http://www.microsoft.com/downloads/details.aspx?familyid=85d8701d-f8c7-4079-8a21-a3a9d5ba71ce Windows Server 2008 for Itanium-based Systems: http://www.microsoft.com/downloads/details.aspx?familyid=b30ee4f0-850f-4ff3-86a4-663603a0a802 * = (core installation is affected). A restart is required. The Microsoft advisory is available at : http://www.microsoft.com/technet/security/bulletin/ms08-038.mspx
References	http://secunia.com/advisories/30953/ CVE Reference: CVE-2008-1435 http://securitytracker.com/alerts/2008/Jul/1020436.html

Vulnerability Name	7. Microsoft Windows DNS Spoofing Vulnerabilities
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	8 July 2008
Classification	Spoofing
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1454
Affected Products	Microsoft Windows 2000 Advanced Server Microsoft Windows 2000 Datacenter Server Microsoft Windows 2000 Professional Microsoft Windows 2000 Server Microsoft Windows 2003 Datacenter Edition Microsoft Windows 2003 Enterprise Edition Microsoft Windows 2003 Standard Edition Microsoft Windows 2003 Web Edition Microsoft Windows Server 2008 Microsoft Windows XP Home Edition Microsoft Windows XP Professional
Description	Two vulnerabilities have been reported in Microsoft Windows, which can be exploited by malicious people to poison the DNS cache. 1) An error in the Windows DNS client and Windows DNS server due to insufficient socket entropy when performing DNS queries can be exploited to poison the DNS cache. 2) An error in the Windows DNS server may cause it to accept records from responses outside of the remote server's authority. This can be exploited via specially crafted responses to DNS requests to poison the DNS cache.
Impact	Spoofing from remote.

Solution	Apply patches. The vendor has issued fixes for both DNS client and DNS server software on the affected platforms. A patch matrix is available in the vendor's advisory: www.microsoft.com/technet/security/Bulletin/MS08-037.mspx A restart is required.
References	CVE Reference: CVE-2008-1454 http://securitytracker.com/alerts/2008/Jul/1020437.html http://secunia.com/advisories/30925/

Vulnerability Name	8. BIND DNS Query Port Entropy Weakness Lets Remote Users Spoof the System
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	8 July 2008
Classification	Spoofing
Severity Rating	Medium http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1447
Affected Products	BIND versions 9.x
Description	The domain name system (DNS) service does not use sufficiently random UDP sockets to process queries. A remote user can send specially crafted DNS queries and responses to the target service to spoof responses and insert records into the DNS cache. This may cause traffic to be redirected to arbitrary IP addresses specified by the remote user. The vendor indicates that the vulnerability exists in the DNS protocol itself, rather than in any particular vendor's implementation. Systems using BIND as a caching resolver are affected.
Impact	A remote user can spoof the DNS service, causing traffic to be redirected to arbitrary hosts.
Solution	The vendor has issued patches (9.5.0-P1, 9.4.2-P1, 9.3.5-P1). New beta releases (9.5.1b1, 9.4.3b2) are also available. The software is available at: http://www.isc.org/index.pl?/menu.pl?sect=sw

References	http://securitytracker.com/alerts/2008/Jul/1020438.html CVE Reference: CVE-2008-1447 http://www.isc.org/index.pl?/sw/bind/index.php

Vulnerability Name	9. BlueZ SDP Processing Vulnerability

Vulnerability Types	Softwares/Systems
Vulnerability Published Date	7 July 2008
Classification	Denial of Service and system access
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2374
Affected Products	BlueZ 3.x
Description	A vulnerability has been reported in BlueZ, which can be exploited by malicious people to cause a DoS (Denial of Service) or to potentially compromise a user's system. The vulnerability is caused due to multiple boundary errors within various functions in src/sdp.c. These can be exploited to trigger a crash or to potentially corrupt memory via specially crafted SDP responses sent by a malicious SDP server. The Bluetooth Session Description Protocol (SDP) packet parser does not properly validate user-supplied input. A local user that can register a service record via a UNIX socket or D-Bus interface may be able to execute arbitrary code with the privileges of the hcid daemon. A remote Bluetooth device with an established trust relationship with the target system can return a specially crafted SDP packet in response to an SDP query from the target system to potentially execute arbitrary code on the target system. The vulnerability is reported in versions prior to 3.34.
Impact	System access from local network.

Solution	Update to bluez-libs 3.35 and bluez-utils 3.35. The vendor has issued a source code patch. The vendor's advisory is available at: http://article.gmane.org/gmane.linux.bluez.devel/15809/
References	http://securitytracker.com/alerts/2008/Jul/1020479.html CVE Reference: CVE-2008-2374 http://secunia.com/advisories/30957/