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. Mac OS X CarbonCore Stack Overflow in Processing Filenames Lets Users Execute Arbitrary Code
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	4 August 2008
Classification	Buffer Overflow
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2320
Affected Products	Versions 10.4.11, 10.5.4
Description	A vulnerability was reported in Mac OS X CarbonCore. A user can cause arbitrary code to be executed on the target system. A remote user can create a specially crafted filename that, when process by the target application, will trigger a stack overflow and execute arbitrary code on the target system.
Impact	Execution of arbitrary code via network. User access via network
Solution	The vendor has issued a fix (Security Update 2008-005), which can be downloaded and installed via Software Update preferences, or from Apple Downloads at: http://www.apple.com/support/downloads/

	For Mac OS X v10.5.4 and Mac OS X Server 10.5.4 The download file is named: "SecUpd2008-005.dmg" Its SHA-1 digest is: 9c4fd4ee59965819427445f6de172c42b223e6e1 For Mac OS X v10.4.11 (Intel) The download file is named: "SecUpd2008-005Intel.dmg" Its SHA-1 digest is: 1ff3242935c98325769b33148a2a8b1e72db567c For Mac OS X v10.4.11 (PPC) The download file is named: "SecUpd2008-005PPC.dmg" Its SHA-1 digest is: 2f56ea4311d5b85de3c494f6fee46360e5b7317e For Mac OS X Server v10.4.11 (Universal) The download file is named: "SecUpdSrvr2008-005Univ.dmg" Its SHA-1 digest is: 256401659308a634cee06b00d1a6ae9dc20b5467 For Mac OS X Server v10.4.11 (PPC) The download file is named: "SecUpdSrvr2008-005PPC.dmg" Its SHA-1 digest is: d310d471bd39df92cb5580e18f356a222824d7d2 The Apple advisory is available at: http://support.apple.com/kb/HT2647
References	http://securitytracker.com/alerts/2008/Aug/1020602.html CVE Reference: CVE-2008-2320 http://secunia.com/advisories/31326/

Vulnerability Name	2. F-Prot Antivirus Attachment Scanning Bug Lets Remote Users Deny Service
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	4 Aug 2008
Classification	Denial of service
Severity Rating	Medium http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-3447
Affected Products	F-Prot Antivirus 6.2.1 4252
Description	A vulnerability was reported in F-Prot Antivirus. A remote or local user can cause denial of service conditions. A remote user can send a specially crafted file that, when scanned by F-Prot on the target user's system, will cause the target scanner to enter an infinite loop.
Impact	Denial of service from local system and from remote.
Solution	There is no effective workaround available. Solution Status: Unpatched
References	http://securitytracker.com/alerts/2008/Aug/1020612.html CVE Reference: CVE-2008-3447 http://secunia.com/advisories/31313/

Vulnerability Name	3. Mac OS X Quick Look Buffer Overflow in Downloading Microsoft Office Files Lets Remote Users Execute Arbitrary Code
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	4 Aug 2008
Classification	Buffer Overflow
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2325
Affected Products	QuickLook in Apple Mac OS X 10.4.11 and 10.5.4
Description	A vulnerability was reported in Mac OS X Quick Look. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can create a specially crafted Microsoft Office file that, when downloaded by the target user, will trigger a buffer overflow and execute arbitrary code on the target system. The code will run with the privileges of the target user. Systems prior to Mac OS X v10.5 are not affected.
Impact	Remote code execution.
Solution	Apple has issued a fix (Security Update 2008-005), which can be downloaded and installed via Software Update preferences, or from Apple Downloads at: http://www.apple.com/support/downloads/ Solution Status: Vendor patch available
References	http://securitytracker.com/alerts/2008/Aug/1020607.html CVE Reference: CVE-2008-2325 http://secunia.com/advisories/31326/

Vulnerability Name	4. Solaris namefs Kernel Module Bug Lets Local Users Gain Kernel Privileges or Deny Service
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	11 July 2008
Classification	Privilege escalation or Denial of Service
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-3450
Affected Products	Sun Solaris 8 through 10
Description	A vulnerability has been reported in Sun Solaris, which can be exploited by malicious, local users to cause a DoS (Denial of Service) or to gain escalated privileges. The vulnerability is caused due to an unspecified error within the namefs kernel module. This can be exploited to cause a system panic or to execute arbitrary code in kernel context. The vulnerability is reported in Solaris 8, 9, and 10 for both the SPARC and x86 platforms.
Impact	Denial of Service via local system, execution of arbitrary code via local system, root access via local system.
Solution	The vendor has issued a fix. SPARC Platform * Solaris 8 with patch 114984-02 or later * Solaris 9 with patch 114971-03 or later * Solaris 10 with patch 136716-01 or later x86 Platform * Solaris 8 with patch 114985-02 or later * Solaris 9 with patch 138570-01 or later

	* Solaris 10 with patch 136717-01 or later The vendor's advisory is available at: http://sunsolve.sun.com/search/document.do?assetkey=1-66-237986-1 Solution Status: Vendor patch available
References	CVE Reference: CVE-2008-3450 http://securitytracker.com/alerts/2008/Aug/1020616.html http://secunia.com/advisories/31356/

Vulnerability Name	5. WS_FTP Pro Format String Bug Lets Remote Users Execute Arbitrary Code
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	20 August 2008
Classification	Format string bug
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-3734
Affected Products	Ipswitch WS_FTP Home 2007.0.0.2 and WS_FTP Professional 2007.1.0.0
Description	A vulnerability was reported in WS_FTP Pro. A remote user can execute arbitrary code on the target system. A remote server can return a specially crafted response to the target client to trigger a format string flaw and execute arbitrary code on the target system. The original advisory is available at: http://milw0rm.com/exploits/6257
Impact	System access from remote
Solution	The vendor has issued hotfixes for some versions. WS_FTP Professional 2007.1 Hotfix 1 (full English version only): http://www.ipswitch.com/support/ws_ftp/releases/wsp20071hf1.asp WS_FTP Home 2007 Hotfix 1 for version 2007.0.0.2 (full English version only): http://www.ipswitch.com/support/ws_ftp/home/releases/wsh2007hf1.asp Connect to trusted servers only.

References	http://secunia.com/advisories/31504/ CVE Reference: CVE-2008-3734 http://securitytracker.com/alerts/2008/Aug/1020714.html

Vulnerability Name	6. Windows nslookup Bug May Let Remote Users Execute Arbitrary Code
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	19 August 2008
Classification	Remote code execution
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-3648
Affected Products	nslookup.exe in Microsoft Windows XP SP2
Description	A vulnerability was reported in nslookup on Microsoft Windows XP. A remote user may be able to cause arbitrary code to be executed on the target user's system. When the target user enters an nslookup zone transfer command, the remote DNS server can return a specially crafted response to execute arbitrary code on the target system. Other commands may be affected. The original advisory is available at: http://packetstormsecurity.org/0808-advisories/Nslookup-Crash.txt The report notes that this vulnerability is being actively exploited.
Impact	A remote server can return a response to a user-generated nslookup command that, when processed by the target nslookup application, will execute arbitrary code on the target user's system.
Solution	No solution was available at the time of this entry

References	http://securitytracker.com/alerts/2008/Aug/1020711.html CVE Reference: CVE-2008-3648 http://packetstormsecurity.org/0808-advisories/Nslookup-Crash.txt

Vulnerability Name	7. Visual Studio Buffer Overflow in 'Msmask32.ocx' ActiveX Control Lets Remote Users Execute Arbitrary Code
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	19 August 2008
Classification	Buffer Overflow
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-3704
Affected Products	Microsoft Visual Studio 6 Enterprise Microsoft Visual Studio 6 Professional Microsoft Visual Studio 6 Standard
Description	A vulnerability has been reported in Microsoft Visual Studio, which can potentially be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error in the Masked Edit ActiveX control (Msmask32.ocx). This can be exploited to cause a stack-based buffer overflow by tricking a user into e.g. visiting a malicious website, which initializes the object with an overly long "Mask" parameter. Successful exploitation may allow execution of arbitrary code. The vulnerability is reported in Msmask32.ocx version 6.0.81.69 included in Microsoft Visual Studio 6.0. Other versions may also be affected.
Impact	Denial of Service and system access from remote.
Solution	The vulnerability is reportedly fixed in Msmask32.ocx version 6.0.84.18. Set the kill-bit for the affected ActiveX control.

References	CVE Reference: CVE-2008-3704 http://securitytracker.com/alerts/2008/Aug/1020710.html http://secunia.com/advisories/31498/

Vulnerability Name	8. Joomla! Password Reset Bug Lets Remote Users Reset a Password
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	13 August 2008
Classification	Security bypass
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-3681
Affected Products	Joomla! versions 1.5 - 1.5.5
Description	The vulnerability is caused due to improper access restriction in components/com_user/models/reset.php. This can be exploited to bypass the authentication mechanism and change the password of the user with the lowest ID (typically the administrator), without having valid user credentials. The vulnerability is reported in all 1.5.x versions prior to 1.5.6.
Impact	Security bypass, manipulation of data from remote.
Solution	The vendor has issued a fixed version (1.5.6). The vendor's advisory is available at: http://developer.joomla.org/security/news/241-20080801-core-password-remind-functionality.html
References	http://securitytracker.com/alerts/2008/Aug/1020687.html CVE Reference: CVE-2008-3681

	http://secunia.com/advisories/31457/

Vulnerability Name	9. Solaris Kernel Lets Local Users Establish Covert Channels
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	28 August 2008
Classification	Covert channel
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-3875
Affected Products	Sun Solaris 8 through 10 and OpenSolaris before snv_90
Description	A vulnerability has been reported in Sun Solaris, which can be exploited by malicious, local users to bypass certain security restrictions. The vulnerability is caused due to an error within the Solaris kernel related to system calls. This can be exploited to establish a covert communication channel between two unprivileged processes, thus bypassing e.g. the multi-level security policy in Solaris Trusted Extensions or the isolation policy of zones(5) or chroot(2). The vulnerability is reported in Solaris 8, 9, 10 for both the SPARC and x86 platforms.
Impact	Provides administrator access, Allows complete confidentiality, integrity, and availability violation; Allows unauthorized disclosure of information;

	Allows disruption of service.
Solution	The vendor has issued the following fixes. SPARC Platform * Solaris 8 with patch 117350-56 or later * Solaris 9 with patch 122300-30 or later * Solaris 10 with patch 137111-05 or later * OpenSolaris based upon builds snv_01 through snv_90 or later x86 Platform * Solaris 8 with patch 117351-56 or later * Solaris 9 with patch 122301-30 or later * Solaris 10 with patch 137112-05 or later * OpenSolaris based upon builds snv_90 or later The vendor's advisory is available at: http://sunsolve.sun.com/search/document.do?assetkey=1-66-240706-1
References	CVE Reference: CVE-2008-3875 http://secunia.com/advisories/31667/ http://securitytracker.com/alerts/2008/Aug/1020780.html

Vulnerability Name	10. HP Enterprise Discovery Unspecified Bug Lets Remote Authenticated Users Gain Elevated Privileges
Vulnerability Types	Softwares/Systems
Vulnerability Published Date	27 August 2008
Classification	Privilege escalation
Severity Rating	High http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-3538
Affected Products	HP Enterprise Discovery 2.x
Description	Unspecified vulnerability in HP Enterprise Discovery 2.0 through 2.52 on Windows allows remote authenticated users to execute arbitrary code via unknown vectors.
Impact	A remote authenticated user can gain elevated privileges on the target system.
Solution	Apply patches (please see vendor advisory for details). http://support.openview.hp.com/selfsolve/patches Vendor advisory is available at: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01508161
References	CVE Reference: CVE-2008-3538 http://secunia.com/advisories/31616/ http://securitytracker.com/alerts/2008/Aug/1020760.html