



Contents

ChemStore B.04.02 SP1	2
ChemStore B.04.02	5
ChemStore B.04.01	8
ChemStore B.03.03	11
Microsoft Hot fixes 2010	16
Microsoft Hot fixes 2009	19
Microsoft Hot fixes 2008	25
Microsoft Hot fixes 2007	34

ChemStore B.04.02 SP1

Rev. B.04.02 SP1		ChemStore Stand-alone	ChemStore Client	Database server	Terminal server
ChemStation (LC, LC/MSD, GC, CE, CE/MSD, A/D)	B.04.01	●	●	✘	●
	B.04.01 SP1	✓	✓	✘	✓
	B.04.02	●	●	✘	●
	B.04.02 DSP 1	●	●	✘	●
	B.04.02 DSP 2	✓	✓	✓	✓
	B.04.02 SP 1	✓	✓	✓	✓
Windows XP Professional					
+ Service Pack	SP2	✘	✘	✘	✘
	SP3	✓	✓	✘	✘
Windows Vista					
+ Service Pack	SP 1	●	●	✘	✘
	SP2	✓	✓	✘	✘
Windows 2003 Server / Adv. Server					
+ Service Pack	SP2	●	●	✓	✓
+ Terminal Services		-	-	●	✓
+ Clustering Services		-	-	●	●
Windows 2003 R2 Server / Adv. Server 32 bit					

● Not tested ○ Currently under testing ✓ Tested and fully supported ! Limited support ✘ Not supported



Rev. B.04.02 SP1		ChemStore Stand-alone	ChemStore Client	Database server	Terminal server
+ Service Pack	SP2	●	●	✓	✓
+ Terminal Services		-	-	●	✓
+ Clustering Services		-	-	●	●
Windows 2003 R2 Server / Adv. Server 64 bit		●	●	●	●
MS Internet Explorer	6.0 SP2	✗	✗	✗	✗
	7.0	✓	✓	✓	✓
	8.0	✓	✓	✓	✓
Internet Information Server		-	-	6.0 for W2003	6.0 for W2003
MDAC		2.8	2.8	2.8	2.8
Java Runtime	1.6.0 07-b06	●	●	●	●
	1.6.0 17-b04	●	✓	✓	✓
	1.6.0 19	●	✓	✓	✓
	1.6.0 20	●	✓	✓	✓
Oracle 10g Release 2					
+ RDBMS	10.2.0.3	✗	✗	✗	✗
	10.2.0.4	✗	✗	✓	✗
+ Client	10.2.0.4	●	✓	●	✓

● Not tested ○ Currently under testing ✓ Tested and fully supported ! Limited support ✗ Not supported

Rev. B.04.02 SP1		ChemStore Stand-alone	ChemStore Client	Database server	Terminal server
+ OLE DB Provider	10.2.0.4	●	✓	●	●
+ OLCritical Patch update	Oct. 2009	●	✓	✓	✓
	Apr 2010	●	✓	✓	✓
+ Oracle Fail Safe (OFS)		-	-	●	✗
+ Oracle Transparent Failover (TAF)		-	-	✗	✗
+ Real Application Clustering (RAC)		-	-	✗	✗
Citrix Terminal Server		✗	✗	✗	✓
Citrix Metaframe XP		✗	✗	✗	✗
Citrix Presentation server 4.5 or higher Advanced Ed.		✗	✗	✗	✓
Citrix Presentation server 4.5 or higher Enterprise Ed.		✗	✗	✗	✓
Citrix Client		✗	✓	✗	✗
Unix		✗	✗	✓ ¹	✗
HPUX 11.11 (11i), 32 or 64-bit		-	-	✓	✗
HPUX 11.20 or higher		-	-	●	✗
Sun Solaris		-	-	●	✗

Notes
¹ ChemStore archive server service is not supported on UNIX. This service needs to be operated on a Windows operating system.

ChemStore B.04.02

Rev. B.04.02		ChemStore Stand-alone	ChemStore Client	Database server	Terminal server
ChemStation (LC, LC/MSD, GC, CE, CE/MSD, A/D)	B.04.01	✓	✓	✗	✓
	B.04.01 SP1	✓	✓	✗	○
Windows XP Professional					
+ Service Pack	SP2	✗	✗	✗	✗
	SP3	✓	✓	✗	✗
Windows Vista					
+ Service Pack	SP 1	✓	✓	✗	✗
	SP2	○	○	✗	✗
Windows 2003 Server / Adv. Server					
+ Service Pack	SP2	●	●	✓	✓
+ Terminal Services		-	-	●	✓
+ Clustering Services		-	-	●	●
Windows 2003 R2 Server / Adv. Server 32 bit					
+ Service Pack	SP2	●	●	✓	✓
+ Terminal Services		-	-	●	✓
+ Clustering Services		-	-	●	●

● Not tested ○ Currently under testing ✓ Tested and fully supported ! Limited support ✗ Not supported

Windows 2003 R2 Server / Adv. Server 64 bit		●	●	●	●
MS Internet Explorer	6.0 SP2	✓	✓	✓	✓
	7.0	✓	✓	✓	✓
	8.0	○	○	○	○
Internet Information Server		-	-	6.0 for W2003	6.0 for W2003
MDAC		2.8	2.8	2.8	2.8
Java Runtime	1.6.0 07-b06	●	✓	✓	✓
Oracle 10g Release 2					
+ RDBMS	10.2.0.3	✗	✗	✗	✗
	10.2.0.4	✗	✗	✓ ¹	✗
+ Client	10.2.0.4	●	✓	●	✓
+ OLE DB Provider	10.2.0.4	●	✓	●	●
+ Oracle Fail Safe (OFS)		-	-	●	✗
+ Oracle Transparent Failover (TAF)		-	-	✗	✗
+ Real Application Clustering (RAC)		-	-	✗	✗
Citrix Terminal Server		✗	✗	✗	✓

Citrix Metaframe XP	x	x	x	x
Citrix Presentation server 4.5 or higher Advanced Ed.	x	x	x	✓
Citrix Presentation server 4.5 or higher Enterprise Ed.	x	x	x	✓
Citrix Client	x	✓	x	x
Unix	x	x	✓ ³	x
HPUX 11.11 (11i), 32 or 64-bit	-	-	✓	x
HPUX 11.20 or higher	-	-	●	x
Sun Solaris	-	-	●	x

Notes

¹ Oracle Enterprise Edition is supported with ChemStore server, however it has not been tested.

² Oracle Standard Edition is tested and supported with ChemStore

³ ChemStore archive server service is not supported on UNIX. This service needs to be operated on a Windows operating system.

ChemStore B.04.01

Rev. B.04.01		ChemStore Stand-alone	ChemStore Client	Database server	Terminal server
ChemStation (LC, LC/MSD, GC, CE, CE/MSD, A/D)	B.03.01 SR 1 or 1.1	✘	✘	✘	✘
	B.03.02 SR2	✓	✓	●	○
Windows XP Professional					
+ Service Pack	SP2	✓	✓	✘	✘
	SP3	●	●	✘	✘
Windows Vista		✘	✘	✘	✘
Windows 2003 Server / Adv. Server					
+ Service Pack	SP2	●	●	✓	○
+ Terminal Services		-	-	●	○
+ Clustering Services		-	-	●	●
Windows 2003 R2 Server / Adv. Server 32 bit					
+ Service Pack	SP1	●	●	●	●
	SP2	●	●	✓	○
+ Terminal Services		-	-	●	○

+ Clustering Services		-	-	●	●
Windows 2003 R2 Server / Adv. Server 64 bit		●	●	●	●
MS Internet Explorer	6.0 SP2	✓	✓	✓	○
	7.0	✓	✓	✓	○
Internet Information Server		-	-	6.0 for W2003	6.0 for W2003
MDAC		2.8	2.8	2.8	2.8
Java Runtime	1.6.0_02-b06	●	✓	✓	○
	1.6.0 03-b07	●	✓	✓	○
Oracle 10g Release 2					
+ RDBMS	10.2.0.1	✗	✗	✗	✗
	10.2.0.2	✗	✗	✗	✗
	10.2.0.3	●	●	✓ ¹	✗
	6637237 (*)	●	●	✓	✗
+ Client	10.2.0.3	●	✓	●	○
	5699495 (#)	●	✓	●	○ !
+ OLE DB Provider	10.2.0.3	●	✓	●	●
+ Oracle Fail Safe (OFS)		-	-	●	✗

+ Oracle Transparent Failover (TAF)	-	-	✘	✘
+ Real Application Clustering (RAC)	-	-	✘	✘
Citrix Terminal Server	✘	✘	✘	○
Citrix Metaframe XP a	✘	✘	✘	○
Citrix Metaframe XP s	✘	✘	✘	○
Citrix Metaframe XP e	✘	✘	✘	○
Citrix Client	✘	○	✘	✘
Unix	✘	✘	✓ ³	✘
HPUX 11.11 (11i), 32 or 64-bit	-	-	✓	✘
HPUX 11.20 or higher	-	-	●	✘
Sun Solaris	-	-	●	✘

Notes
¹ Oracle Enterprise Edition is supported with ChemStore server, however it has not been tested.
² Oracle Standard Edition is tested and supported with ChemStore
³ ChemStore archive server service is not supported on UNIX. This service needs to be operated on a Windows operating system.
 *) Oracle Critical Patch update January 2008
 #) Oracle ODBC driver patch

ChemStore B.03.03

Rev. B.03.03 SR 3		ChemStore Stand-alone	ChemStore Client	Database server	Terminal server
ChemStation (LC, LC/MSD, GC, CE, CE/MSD, A/D)	B.02.01 SR2	✓	✓	●	✓
	B.03.01 SR 1 or 1.1	✓	✓	●	●
	B.03.02 SR2	✗	! ⁹	●	●
Windows 2000 Server / Adv. Server					
+ Service Pack	SP4	-	-	✓	✓
+ Terminal Services		✗	✗	●	✓
+ Clustering Services		✗	✗	●	●
Windows 2000 Professional					
+ Service Pack	SP4	✓	✓	✗	✗
Windows XP Professional					
+ Service Pack	SP1a	●	●		
	SP2	✓	✓	✗	✗
Windows Vista		✗	✗	✗	✗
Windows 2003 Server / Adv. Server					

+ Service Pack	SP1	●	●	!	✓
	SP2	●	●	✓	✓
+ Terminal Services		-	-	●	✓
+ Clustering Services		-	-	●	●
Windows 2003 R2 Server / Adv. Server					
+ Service Pack	SP1	●	●	●	●
	SP2	●	●	✓	✓
+ Terminal Services		-	-	●	✓
+ Clustering Services		-	-	●	●
MS Internet Explorer	5.5	●	●	●	●
	6.0 or 6.0 SP1	✓	✓	✓	✓
	7.0	! 5	! 5	! 5	○
Internet Information Server		-	-	5.0 for W2K 6.0 for W2003 6.0 for W2003	5.0 for W2K 6.0 for W2003
MDAC		2.8	2.8	2.8	2.8
Java Runtime	1.5.0_04	●	!	!	!
	1.5.0_06-b05	●	!	!	!
	1.5.0_10-b03	●	!	!	!

	1.5.0_11-b03	●	✓	✓	✓
	1.6.0 03-b05	●	✓	✓	✓
Oracle 9i Release 2					
+ RDBMS	9.2.0.6	✘	✘	✘	✘
	9.2.0.7	●	●	✓	✓
	9.2.0.8 (4)	●	●	!	!
	4751528 (*)	●	●	✓	✓
	5064365(+)	●	●	!	!
	5250980(x)	●	●	!	!
	5500873(!)	●	●	!	!
	5654905 (-)	●	●	!	!
	5047902 (0)	●	●	✓	✓
	5907274 (6)	●	●	!	!
	6146759 (7)	●	●	!	!
	6130293 (8)	●	●	!	!
	6417013 (9)	●	●	!	!

+ Client	9.2.0.7	●	✓	✓	✓
	9.2.0.8 (4)	●	!	!	!
+ OLE DB Provider	9.2.0.2	●	✗	✗	✗
	9.2.0.4		✓	✓	✓
+ Oracle Fail Safe (OFS)		-	-	✗	✗
+ Oracle Transparent Failover (TAF)		-	-	✗	✗
+ Real Application Clustering (RAC)		-	-	✗	✗
Citrix Terminal Server		✗	✗	✗	✓
Citrix Metaframe XP a		✗	✗	✗	✓
Citrix Metaframe XP s		✗	✗	✗	✗
Citrix Metaframe XP e		✗	✗	✗	✓
Citrix Client		✗	✓	✗	✗
Unix		✗	✗	✓ ³	✗
HPUX 11.11 (11i), 32 or 64-bit		-	-	✓	✗
HPUX 11.20 or higher		-	-	●	✗
Sun Solaris		-	-	●	✗

**Notes**

¹ Oracle Enterprise Edition is supported with ChemStore server, however it has not been tested.

² Oracle Standard Edition is tested and supported with ChemStore

³ ChemStore archive server service is not supported on UNIX. This service needs to be operated on a Windows operating system.

⁴ Upgrade installations only.

⁵ Only after installing ChemStore server B.03.03 Patch 02 on the ChemStore server. Co-execution with ChemStation has not been tested.

* Oracle 9.2.0.7.0 Patch 5: 4751528 (January 2006)

+ Oracle 9.2.0.7.0 Patch 9: 5064365 (April 2006) Note: The patch must not be installed prior to the ChemStore server database creation.

Upgrading an existing ChemStore server database is possible.

x Oracle 9.2.0.7.0 Patch 12: 5250980 (July 2006) Note: The patch must not be installed prior to the ChemStore server database creation.

Upgrading an existing ChemStore server database is possible.

! Oracle 9.2.0.7.0 Patch 14: 5500873 (October 2006) Note: The patch must not be installed prior to the ChemStore server database creation. Upgrading an existing ChemStore server database is possible.

- Oracle 9.2.0.7.0 Patch 15: 5654905 (January 2007) Note: The patch must not be installed prior to the ChemStore server database creation. Upgrading an existing ChemStore server database is possible.

o Oracle 9.2.0.7.0 Interim Patch for bug 5047902 JVM TIMEZONE COMMONWEALTH GAME FORCING MOVE OF TIMEZONE CHAGE

⁶ Oracle 9.2.0.7.0 Patch 16: 5907274 (April 2007) Note: The patch must not be installed prior to the ChemStore server database creation.

Upgrading an existing ChemStore server database is possible.

⁷ Oracle DB 9.2.0.7.0 Patch 17: 6146759 (July 2007) Note: The patch must not be installed prior to the ChemStore server database creation. Upgrading an existing ChemStore server database is possible.

⁸ Oracle 9.2.0.8.0 Patch 10: 6130293 (July 2007) Note: The patch must not be installed prior to the ChemStore server database creation. Upgrading an existing ChemStore server database is possible.

⁸ Oracle 9.2.0.8.0 Patch 12: 6417013 (October 2007) Note: The patch must not be installed prior to the ChemStore server database creation. Upgrading an existing ChemStore server database is possible.

⁹ See Service Note G2181BA-76



Microsoft Hot fixes 2010

The following table shows the list of tested and supported Microsoft® Windows® security hot fixes. Certain hot fixes are not tested by Agilent due to incompatibilities of the affected Microsoft application with the ChemStation Plus applications or in cases where the Microsoft base application has not been tested in combination with ChemStation Plus (e.g. Microsoft® Publisher®). Installation of non-tested applications or Security Fixes is at own risk.

If you intend to apply non-tested hot fixes in your certified production environment, Agilent recommends that you test the hot fixes in a test environment that you setup to represent your production environment.

Information about the latest Microsoft® hotfixes can be found on [here](#).

(Patch #) / Bulletin #	Severity	Date	ChemStore version			Notes
			B.04.02	B.04.01	B.03.03 SR3	
Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (978213) : MS10-031	Critical	May 11, 2010	✓	✓	●	
Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542) : MS10-030	Critical	May 11, 2010	✓	✓	●	
Vulnerability in Windows ISATAP Component Could Allow Spoofing (978338) : MS10-029	Moderate	Apr 13, 2010	✓	✓	●	
Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (980094) : MS10-028	Important	Apr 13, 2010	✓	✓	●	
Vulnerability in Windows Media Player Could Allow Remote Code Execution (979402) : MS10-027	Critical	Apr 13, 2010	✓	✓	●	
Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (977816) : MS10-026	Critical	Apr 13, 2010	✓	✓	●	
Vulnerability in Microsoft's Windows Media Services Could Allow Remote Code Execution (980858) : MS10-025	Critical	Apr 13, 2010	✗	✗	✗	
Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) : MS10-024	Important	Apr 13, 2010	✓	✓	●	
Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (981160) : MS10-023	Important	Apr 13, 2010	✓	✓	●	

Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169): MS10-022	Important	Apr 13, 2010	✓	✓	●	
Vulnerabilities in Windows Kernel could allow Elevation of Privilege (979683): MS10-021	Important	Apr 13, 2010	✓	✓	●	
Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232): MS10-020	Critical	Apr 13, 2010	✓	✓	●	
Vulnerabilities in Windows Could Allow Remote Code Execution (981210): MS10-019	Critical	Apr 13, 2010	✓	✓	●	
Cumulative Security Update for Internet Explorer (980182): MS10-018	Critical	Mar 30, 2010	✓	✓	●	
Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150): MS10-017	Important	Mar 9, 2010	✓	✓	●	
Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (975561): MS10-016	Important	Mar 9, 2010	●	●	●	
Vulnerabilities in Windows Kernel could allow Elevation of Privilege (977165): MS10-015	Important	Feb 9, 2010	✓	✓	●	
Vulnerability in Kerberos Could Allow Denial of Service (977290): MS10-014	Important	Feb 9, 2010	✓	✓	●	
Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935): MS10-013	Critical	Feb 9, 2010	●	●	●	
Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468): MS10-012	Important	Feb 9, 2010	✓	✓	●	
Vulnerabilities in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (978037): MS10-011	Important	Feb 9, 2010	●	●	●	
Vulnerability in Windows Hyper-V Could Allow Denial of Service (977894): MS10-010	Important	Feb 9, 2010	●	●	●	
Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145): MS10-009	Critical	Feb 9, 2010	✓	✓	●	
Cumulative Security Update of ActiveX Kill Bits (978262): MS10-008	Critical	Feb 9, 2010	✓	✓	●	
Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (975713): MS10-007	Critical	Feb 9, 2010	✓	✓	●	
Vulnerabilities in SMB Client Could Allow Remote Code	Critical	Feb 9, 2010	✓	✓	●	



<u>Execution (978251): MS10-006</u>						
<u>Vulnerability in Microsoft Paint Could Allow Remote Code Execution (978706): MS10-005</u>	Moderate	Feb 9, 2010	✓	✓	●	
<u>Vulnerabilities in Microsoft Office PowerPoint could allow Remote Code Execution (975416): MS10-004</u>	Important	Feb 9, 2010	✓	✓	●	
<u>Vulnerability in Microsoft Office (MSO) Could Allow Remote Code Execution (978214): MS10-003</u>	Important	Feb 9, 2010	✓	✓	●	
<u>Critical Cumulative Security Update for Internet Explorer (978207): MS10-002</u>	Critical	Jan 21, 2010	✓	✓	●	
<u>Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270): MS10-001</u>	Critical	Jan 12, 2010	✓	✓	●	



Microsoft Hot fixes 2009

Last Updated: 12-Nov-09

The following table shows the list of tested and supported Microsoft® Windows® security hot fixes. Certain hot fixes are not tested by Agilent due to incompatibilities of the affected Microsoft application with the ChemStation Plus applications or in cases where the Microsoft base application has not been tested in combination with ChemStation Plus (e.g. Microsoft® Publisher®). Installation of non-tested applications or Security Fixes is at own risk.

If you intend to apply non-tested hot fixes in your certified production environment, Agilent recommends that you test the hot fixes in a test environment that you setup to represent your production environment.

Information about the latest Microsoft® hotfixes can be found on [here](#).

(Patch #) / Bulletin #	Severity	Date	ChemStore version			Notes
			B.04.02	B.04.01	B.03.03 SR3	
Vulnerability in Microsoft Office Project Could Allow Remote Code Execution (967183) : MS09-074	Critical	Dec 8, 2009	✓	✓	✓	
Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (975539) : MS09-073	Important	Dec 8, 2009	✓	✓	✓	
Cumulative Security Update for Internet Explorer (974455) : MS09-072	Critical	Dec 8, 2009	✓	✓	✓	
Vulnerability on Internet Authentication Service Could Allow Remote Code Execution (974318) : MS09-071	Critical	Dec 8, 2009	✓	✓	✓	
Vulnerabilities in Active Directory Federation Services Could Allow Remote Code Execution (971726) : MS09-070	Important	Dec 8, 2009	✓	✓	✓	
Vulnerability in Local Security Subsystem Authority Service Could Allow Denial of Service (974392) : MS09-069	Important	Dec 8, 2009	✓	✓	✓	
Vulnerability in Microsoft Office Word Could Allow Remote Code Execution (976307) : MS09-068	Important	Nov 11, 2009	✓	✓	✓	
Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652) : MS09-067	Important	Nov 11, 2009	✓	✓	✓	

<u>Vulnerability in Active Directory Could Allow Denial of Service (973309): MS09-066</u>	Important	Nov 11, 2009	✓	✓	✓	
<u>Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947): MS09-065</u>	Critical	Nov 11, 2009	✓	✓	✓	
<u>Vulnerability in License Logging Server Could Allow Remote Code Execution (974783): MS09-064</u>	Critical	Nov 11, 2009	✓	✓	✓	
<u>Vulnerability in Web Service on Devices Could Allow Remote Code Execution (973565): MS09-063</u>	Critical	Nov 11, 2009	✓	✓	✓	
<u>Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488): MS09-062</u>	Critical	Oct 14, 2009	✓	✓	✓	
<u>Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution (974378): MS09-061</u>	Critical	Oct 14, 2009	✓	✓	✓	
<u>Vulnerabilities in Microsoft Active Template Library (ATL) ActiveX Controls for Microsoft Office Could Allow Remote Code Execution (973965): MS09-060</u>	Critical	Oct 14, 2009	✓	✓	✓	
<u>Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (975467): MS09-059</u>	Important	Oct 14, 2009	✓	✓	✓	
<u>Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (971486): MS09-058</u>	Important	Oct 14, 2009	✓	✓	✓	
<u>Vulnerability in Indexing Service Could Allow Remote Code Execution (969059): MS09-057</u>	Important	Oct 14, 2009	✓	✓	✓	
<u>Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571): MS09-056</u>	Important	Oct 14, 2009	✓	✓	✓	
<u>Cumulative Security Update of ActiveX Kill Bits (973525): MS09-055</u>	Critical	Oct 14, 2009	✓	✓	✓	
<u>Cumulative Security Update for Internet Explorer (974455): MS09-054</u>	Critical	Oct 14, 2009	✓	✓	✓	
<u>Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution (975254): MS09-053</u>	Important	Oct 14, 2009	✓	✓	✓	
<u>Vulnerability in Windows Media Player Could Allow Remote Code Execution (974112): MS09-052</u>	Critical	Oct 14, 2009	✓	✓	✓	
<u>Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution (975682): MS09-051</u>	Critical	Oct 14, 2009	✓	✓	✓	



<u>Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517): MS09-050</u>	Critical	Oct 14, 2009	✓	✓	✓	
<u>Vulnerability in Wireless LAN AutoConfig Service Could Allow Remote Code Execution (970710): MS09-049</u>	Critical	Sep 8, 2009	✓	✓	✓	
<u>Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723): MS09-048</u>	Critical	Sep 8, 2009	✓	✓	✓	
<u>Vulnerabilities in Windows Media Format Could Allow Remote Code Execution (973812): MS09-047</u>	Critical	Sep 8, 2009	✓	✓	✓	
<u>Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (956844): MS09-046</u>	Critical	Sep 8, 2009	✓	✓	✓	
<u>Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution (971961): MS09-045</u>	Critical	Sep 8, 2009	✓	✓	✓	
<u>Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (970927): MS09-044</u>	Critical	Aug 11, 2009	✓	✓	✓	
<u>Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (957638): MS09-043</u>	Critical	Aug 11, 2009	✓	✓	✓	
<u>Vulnerability in Telnet Could Allow Remote Code Execution (960859): MS09-042</u>	Important	Aug 11, 2009	✓	✓	✓	
<u>Vulnerability in Workstation Service Could Allow Elevation of Privilege (971657): MS09-041</u>	Important	Aug 11, 2009	✓	✓	✓	



<u>Vulnerability in Message Queuing Could Allow Elevation of Privilege (971032): MS09-040</u>	Important	Aug 11, 2009	✓	✓	✓	
<u>Vulnerabilities in WINS Could Allow Remote Code Execution (969883): MS09-039</u>	Critical	Aug 11, 2009	✓	✓	✓	
<u>Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (971557): MS09-038</u>	Critical	Aug 11, 2009	✓	✓	✓	
<u>Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908): MS09-037</u>	Critical	Aug 11, 2009	✓	✓	✓	
<u>Vulnerability in ASP.NET in Microsoft Windows Could Allow Denial of Service (970957): MS09-036</u>	Important	Aug 11, 2009	✓	✓	✓	
<u>Vulnerabilities in Visual Studio Active Template Library Could Allow Remote Code Execution (969706): MS09-035</u>	Moderate	Jul 28, 2009	✓	✓	✓	
<u>Cumulative Security Update for Internet Explorer (972260): MS09-034</u>	Critical	Jul 28, 2009	✓	✓	✓	
<u>Vulnerability in Virtual PC and Virtual Server could lead to Elevation of Privilege (969856): MS09-033</u>	Important	Jul 14, 2009	✓	✓	✓	
<u>Cumulative Security Update of ActiveX Kill Bits (973346): MS09-032</u>	Critical	Jul 14, 2009	✓	✓	✓	
<u>Vulnerability in Microsoft ISA Server 2006 Could Cause Elevation of Privilege (970953): MS09-031</u>	Important	Jul 14, 2009	✓	✓	✓	
<u>Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (969516): MS09-030</u>	Important	Jul 14, 2009	✓	✓	✓	
<u>Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (961371): MS09-029</u>	Critical	Jul 14, 2009	✓	✓	✓	
<u>Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (971633): MS09-028</u>	Critical	Jul 14, 2009	✓	✓	✓	

<u>Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (969514): MS09-027</u>	Critical	Jun 9, 2009	✓	✓	✓	
<u>Vulnerability in RPC Could Allow Elevation of Privilege (970238): MS09-026</u>	Important	Jun 9, 2009	✓	✓	✓	
<u>Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537): MS09-025</u>	Important	Jun 9, 2009	✓	✓	✓	
<u>Vulnerability in Microsoft Works Converters Could Allow Remote Code Execution (957632): MS09-024</u>	Critical	Jun 9, 2009	✓	✓	✓	
<u>Vulnerability in Windows Search Could Allow Information Disclosure (963093): MS09-023</u>	Moderate	Jun 9, 2009	✓	✓	✓	
<u>Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501): MS09-022</u>	Critical	Jun 9, 2009	✓	✓	✓	
<u>Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462): MS09-021</u>	Critical	Jun 9, 2009	✓	✓	✓	
<u>Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483): MS09-020</u>	Important	Jun 9, 2009	✓	✓	✓	
<u>Cumulative Security Update for Internet Explorer (969897): MS09-019</u>	Critical	Jun 9, 2009	✓	✓	✓	
<u>Vulnerabilities in Active Directory Could Allow Remote Code Execution (971055): MS09-018</u>	Critical	Jun 9, 2009	✓	✓	✓	
<u>Vulnerabilities in Microsoft Office Powerpoint Could Allow Remote Code Execution (967340): MS09-017</u>	Critical	May 12, 2009	✓	✓	✓	
<u>Vulnerabilities in Microsoft ISA Server and Forefront Threat Management Gateway (Medium Business Edition) Could Cause Denial of Service (961759): MS09-016</u>	Important	Apr 14, 2009	✓	✓	✓	
<u>Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426): MS09-015</u>	Moderate	Apr 14, 2009	✓	✓	✓	
<u>Cumulative Security Update for Internet Explorer (963027): MS09-014</u>	Critical	Apr 14, 2009	✓	✓	✓	
<u>Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803): MS09-013</u>	Critical	Apr 14, 2009	✓	✓	✓	
<u>Vulnerabilities in Windows Could Allow Elevation of Privilege (959454): MS09-012</u>	Important	Apr 14, 2009	✓	✓	✓	
<u>Vulnerability in Microsoft DirectShow Could Allow Remote Code</u>	Critical	Apr 14, 2009	✓	✓	✓	



Execution (961373): MS09-011						
<u>Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (960477): MS09-010</u>	Critical	Apr 14, 2009	✓	✓	✓	
<u>Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557): MS09-009</u>	Critical	Apr 14, 2009	✓	✓	✓	
<u>Vulnerabilities in DNS and WINS Server Could Allow Spoofing (962238): MS09-008</u>	Important	Mar 11, 2009	●	●	●	Win 2003 SP2
<u>Vulnerability in SChannel Could Allow Spoofing (960225): MS09-007</u>	Important	Mar 11, 2009	✓	✓	✓	XP SP 2, Win 2003 SP2, Vista SP1
<u>Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690): MS09-006</u>	Critical	Mar 11, 2009	✓	✓	✓	XP SP 3, Win 2003 SP2, Vista SP1
<u>Vulnerabilities in Microsoft Office Visio Could Allow Remote Code Execution (957634): MS09-005</u>	Important	Feb 10, 2009	●	●	●	Office Visio
<u>Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420): MS09-004</u>	Important	Feb 16, 2009	●	●	●	SQL server
<u>Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution (959239): MS09-003</u>	Critical	Feb 25, 2009	●	●	●	Exchange server
<u>Cumulative Security Update for Internet Explorer (961260): MS09-002</u>	Critical	Feb 16, 2009	✓	✓	✓	Internet Explorer 7
<u>Vulnerabilities in SMB Could Allow Remote Code Execution (958687): MS09-001</u>	Critical	Jan 13, 2009	✓	✓	✓	

Microsoft Hot fixes 2008

Last Updated: 05-Mar-09

The following table shows the list of tested and supported Microsoft Windows security hot fixes. Certain hot fixes are not tested by Agilent due to incompatibilities of the affected Microsoft application with the ChemStation Plus applications (e.g. MS Access 2003) or in cases where the Microsoft base application has not been tested in combination with ChemStation Plus (e.g. Microsoft Publisher). Installation of non-tested applications or Security Fixes is at own risk.

If you intend to apply non-tested hot fixes in your certified production environment, Agilent recommends that you test the hot fixes in a test environment that you setup to represent your production environment.

Bulletin # MS08-	Patch #	Severity	Date	B.04.01	B.03.03 SR3	B.03.02 SR 3	Notes
078	Security Update for Internet Explorer (960714)	Critical	Dec 17, 2008	✓	✓	✓	Internet Explorer 6.0 , 7.0
077	Vulnerability in Microsoft Office SharePoint Server Could Cause Elevation of Privilege (957175)	Important	Dec 9, 2008	●	●	●	SharePoint Server
076	Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807) MS08-076	Important	Dec 9, 2008	✓	✓	✓	Windows Media Player
075	Vulnerabilities in Windows Search Could Allow Remote Code Execution (959349)	Critical	Dec 9, 2008	✓	✓	✓	Windows Server 2008 Windows Vista
074	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (959070)	Critical	Dec 9, 2008	✓	✓	✓	Excel 2007



073	<u>Cumulative Security Update for Internet Explorer (958215)</u>	Critical	Dec 9, 2008	✓	✓	✓	Internet Explorer 6.0 and 7.0
072	<u>Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution(957173)</u>	Critical	Dec 9, 2008	✓	✓	✓	Word
071	<u>Vulnerabilities in GDI Could Allow Remote Code Execution(956802)</u>	Critical	Dec 9, 2008	✓	✓	✓	Windows Server 2003
070	<u>Vulnerabilities in Visual Basic 6.0 Runtime Extended Files (ActiveX Controls) Could Allow Remote Code Execution(932349)</u>	Critical	Dec 9, 2008	✓	✓	✓	Visual Basic 6.0
069	<u>Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (955218)</u>	Critical	Nov 11, 2008	✓	✓	✓	Windows Server 2003
068	<u>Vulnerability in SMB Could Allow Remote Code Execution (957097)</u>	Important	Nov 11, 2008	✓	✓	✓	Windows Server 2003 SP2
067	<u>Vulnerability in Server Service Could Allow Remote Code Execution (958644)</u>	Critical	Oct 23, 2008	✓	✓	✓	Windows Vista SP1
066	<u>Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege (956803)</u>	Important	Oct 14, 2008	✓	✓	✓	Windows XP Service Pack 3
065	<u>Vulnerability in Message Queuing Could Allow Remote Code Execution (951071)</u>	Important	Oct 14, 2008	✓	✓	✓	Windows 2000 SP4
064	<u>Vulnerability in Virtual Address Descriptor Manipulation Could Allow Elevation of Privilege (956841)</u>	Important	Oct 14, 2008	✓	✓	✓	Windows XP Service Pack 3



063	Vulnerability in SMB Could Allow Remote Code Execution (957095)	Important	Oct 14, 2008	✓	✓	✓	Windows Server 2003 SP2
062	Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution (953155):	Important	Oct 14, 2008	✓	✓	✓	Windows Server 2003 SP2 Windows Vista SP1
061	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (954211)	Important	Oct 14, 2008	✓	✓	✓	Windows XP SP2 Windows Server 2003 SP2 Windows Vista SP1
060	Vulnerability in Active Directory Could Allow Remote Code Execution (957280)	Critical	Oct 14, 2008	✓	✓	✓	Windows 2000 SP 4
059	Vulnerability in Host Integration Server RPC Service Could Allow Remote Code Execution (956695)	Critical	Oct 14, 2008	●	●	●	Host Integration Server SP2
058	Cumulative Security Update for Internet Explorer (956390): MS08-058	Critical	Oct 14, 2008	✓	✓	✓	Internet Explorer 6 and 7
057	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (956416): MS08-057	Critical	Oct 14, 2008	✓	✓	✓	Excel
056	Vulnerability in Microsoft Office Could Allow Information Disclosure (957699): MS08-056	Moderate	Oct 14, 2008	✓	✓	✓	Office XP SP3
055	Vulnerability in Microsoft Office Could Allow Remote Code Execution (955047): MS08-055	Critical	Sep 9, 2008	✓	✓	✓	Office System 2007
054	Vulnerability in Windows Media Player Could Allow Remote Code Execution (954154): MS08-054	Critical	Sep 9, 2008	✓	✓	✓	Media Player

053	<u>Vulnerability in Windows Media Encoder 9 Could Allow Remote Code Execution (954156): MS08-053</u>	Critical	Sep 9, 2008	✓	✓	✓	Windows XP SP3
052	<u>Vulnerabilities in GDI+ Could Allow Remote Code Execution (954593): MS08-052</u>	Critical	Sep 9, 2008	✓	✓	✓	Windows XP SP3
051	<u>Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (949785): MS08-051</u>	Critical	Aug 12, 2008	●	●	●	PowerPoint
050	<u>Vulnerability in Windows Messenger Could Allow Information Disclosure (955702): MS08-050</u>	Important	Aug 12, 2008	✓	✓	✓	Windows XP SP3
049	<u>Vulnerability in Event System Could Allow Remote Code Execution (950974): MS08-049</u>	Important	Aug 12, 2008	✓	✓	✓	Windows XP SP3 Windows Server 2003 SP2
048	<u>Security Update for Outlook Express and Windows Mail (951066): MS08-048</u>	Important	Aug 12, 2008	●	●	●	Outlook Express
047	<u>Vulnerability in IPsec Policy Processing Could Allow Information Disclosure (953733): MS08-047</u>	Important	Aug 12, 2008	✓	✓	✓	Windows Vista SP1
046	<u>Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution (952954): MS08-046</u>	Critical	Aug 12, 2008	✓	✓	✓	Windows XP SP3 Windows Server 2003 SP2
045	<u>Cumulative Security Update for Internet Explorer (953838): MS08-045</u>	Critical	Aug 12, 2008	✓	✓	✓	Internet Explorer 6 and 7



044	Vulnerabilities in Microsoft Office Filters Could Allow Remote Code Execution (924090): MS08-044	Critical	Aug 12, 2008	✓	✓	✓	Office 2003 SP2
043	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (954066): MS08-043	Critical	Aug 12, 2008	✓	✓	✓	Excel
042	Vulnerability in Microsoft Word Could Allow Remote Code Execution (955048): MS08-042	Important	Aug 12, 2008	✓	✓	✓	Office XP SP3
041	Vulnerability in the ActiveX Control for the Snapshot Viewer for Microsoft Access Could Allow Remote Code Execution (955617): MS08-041	Critical	Aug 12, 2008	✓	✓	✓	Office
040	Vulnerabilities in Microsoft SQL Server Could Allow Elevation of Privilege (941203): MS08-040	Important	Jul 8, 2008	●	●	●	SQL Server
039	Vulnerabilities in Outlook Web Access for Exchange Server Could Allow Elevation of Privilege (953747): MS08-039	Important	Jul 8, 2008	●	●	●	Exchange Server
038	Vulnerability in Windows Explorer Could Allow Remote Code Execution (950582): MS08-038	Important	Jul 8, 2008	✓	✓	✓	Windows Vista SP1
037	Vulnerabilities in DNS Could Allow Spoofing (953230): MS08-037	Important	Jul 8, 2008	✓	✓	✓	Windows XP SP 3
036	Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service (950762): MS08-036	Important	Jun 10, 2008	✓	✓	✓	Windows XP SP 3,
035	Vulnerability in Active Directory Could Allow Denial of Service (953235): MS08-035	Important	Jun 10, 2008	✓	✓	✓	Windows XP SP 3



034	<u>Vulnerability in WINS Could Allow Elevation of Privilege (948745)</u> : MS08-034	Important	Jun 10, 2008	✓	✓	✓	Windows Server 2003 SP2
033	<u>Vulnerabilities in DirectX Could Allow Remote Code Execution (951698)</u> : MS08-033	Critical	Jun 10, 2008	✓	✓	✓	Windows XP SP 3 Windows Vista SP1
032	<u>Cumulative Security Update of ActiveX Kill Bits (950760)</u> : MS08-032	Moderate	Jun 10, 2008	✓	✓	✓	Windows XP SP 3 Windows Vista SP1
031	<u>Cumulative Security Update for Internet Explorer (950759)</u> : MS08-031	Critical	Jun 10, 2008	✓	✓	✓	IE 6 and 7
030	<u>Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (951376)</u> : MS08-030	Critical	Jun 10, 2008	✓	✓	✓	Windows XP SP 3 Windows Vista SP1
029	<u>Vulnerabilities in Microsoft Malware Protection Engine Could Allow Denial of Service (952044)</u> : MS08-029	Moderate	May 13, 2008	✓	✓	✓	
028	<u>Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution (950749)</u> : MS08-028	Critical	May 13, 2008	✓	✓	✓	Windows XP SP 2
027	<u>Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (951208)</u> : MS08-027	Critical	May 13, 2008	●	●	●	Publisher
026	<u>Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (951207)</u> : MS08-026	Critical	May 13, 2008	✓	✓	✓	Word



025	Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693): MS08-025	Important	Apr 8, 2008	✓	✓	✓	Windows XP SP 3 Windows Vista SP1
024	Cumulative Security Update for Internet Explorer (947864): MS08-024	Critical	Apr 8, 2008	✓	✓	✓	IE 6 and 7
023	Security Update of ActiveX Kill Bits (948881): MS08-023	Critical	Apr 8, 2008	✓	✓	✓	Windows XP SP 3 Windows Vista SP1
022	Vulnerability in VBScript and JScript Scripting Engines Could Allow Remote Code Execution (944338): MS08-022	Critical	Apr 8, 2008	✓	✓	✓	
021	Vulnerabilities in GDI Could Allow Remote Code Execution (948590): MS08-021	Critical	Apr 8, 2008	✓	✓	✓	
020	Vulnerability in DNS Client Could Allow Spoofing (945553): MS08-020	Important	Apr 8, 2008	✓	✓	✓	
019	Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (949032): MS08-019	Important	Apr 8, 2008	●	●	●	Visio
018	Vulnerability in Microsoft Project Could Allow Remote Code Execution (950183): MS08-018	Critical	Apr 8, 2008	●	●	●	Project
017	Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (933103): MS08-017	Critical	Mar 11, 2008	✓	✓	✓	Office 2000 SP 3, Office XP SP3
016	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (949030): MS08-016	Critical	Mar 11, 2008	✓	✓	✓	Office



015	Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (949031) : MS08-015	Critical	Mar 11, 2008	●	●	●	Outlook
014	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (949029) : MS08-014	Critical	Mar 11, 2008				Excel
013	Vulnerability in Microsoft Office Could Allow Remote Code Execution (947108) : MS08-013	Critical	Feb 12, 2008	✓	✓	✓	MS Office
012	Vulnerabilities in Microsoft Office Publisher Could Allow Remote Code Execution (947085) : MS08-012	Critical	Feb 12, 2008	●	●	●	MS Publisher
011	Vulnerabilities in Microsoft Works File Converter Could Allow Remote Code Execution (947081) : MS08-011	Important	Feb 12, 2008	●	●	●	
010	Cumulative Security Update for Internet Explorer (944533) : MS08-010	Critical	Feb 12, 2008	✓	✓	✓	Internet Explorer 6 or 7
009	Vulnerability in Microsoft Word Could Allow Remote Code Execution (947077) : MS08-009	Critical	Feb 12, 2008	✓	✓	✓	MS Word
008	Vulnerability in OLE Automation Could Allow Remote Code Execution (947890) : MS08-008	Critical	Feb 12, 2008	✓	✓	✓	
007	Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026) : MS08-007	Critical	Feb 12, 2008	✓	✓	✓	
006	Vulnerability in Internet Information Services Could Allow Remote Code Execution (942830) : MS08-006	Important	Feb 12, 2008	✓	✓	✓	



005	<u>Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831): MS08-005</u>	Important	Feb 12, 2008	✓	✓	✓	IIS
004	<u>Vulnerability in Windows TCP/IP Could Allow Denial of Service (946456): MS08-004</u>	Important	Feb 12, 2008	✗	✗	✗	MS Vista
003	<u>Vulnerability in Active Directory Could Allow Denial of Service (946538): MS08-003</u>	Important	Feb 12, 2008	✓	✓	✓	
002	<u>Vulnerability in LSASS Could Allow Local Elevation of Privilege (943485): MS08-002</u>	Important	Jan 8, 2008	✓	✓	✓	
001	<u>Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644): MS08-001</u>	Critical	Jan 8, 2008	✓	✓	✓	

Microsoft Hot fixes 2007

The following table shows the list of tested and supported Microsoft Windows security hot fixes. Certain hot fixes are not tested by Agilent due to incompatibilities of the affected Microsoft application with the ChemStation Plus applications (e.g. MS Access 2003) or in cases where the Microsoft base application has not been tested in combination with ChemStation Plus (e.g. Microsoft Publisher). Installation of non-tested applications or Security Fixes is at own risk.

If you intend to apply non-tested hot fixes in your certified production environment, Agilent recommends that you test the hot fixes in a test environment that you setup to represent your production environment.

Bulletin #	Patch #	Severity	Date	B.03.03 SR2	B.03.02 SR 3	B.03.01 SR2	B.02.02	Notes
MS07-069	942615	Critical	Dec 11, 2007	✓	✓	✗	✗	Internet Explorer
MS07-068	941569 and 944275	Critical	Dec 11, 2007	●	●	✗	✗	Media Player
MS07-067	944653	Important	Dec 11, 2007	✓	✓	✗	✗	
MS07-066	943078	Important	Dec 11, 2007	●	●	✗	✗	MS Vista
MS07-065	937894	Important	Dec 11, 2007	✓	✓	✗	✗	
MS07-064	941568	Critical	Dec 11, 2007	●	●	✗	✗	Direct X
MS07-063	942624	Important	Dec 11, 2007	●	●	✗	✗	MS Vista
MS07-062	941672	Important	Nov 13, 2007	✓	✓	✗	✗	Windows 2003 server
MS07-061	943460	Critical	Nov 13, 2007	✓	✓	✗	✗	
MS07-060	942695	Critical	Oct 10, 2007	●	●	✗	✗	MS Office 2000
MS07-059	942017	Important	Oct 10, 2007	●	●	✗	✗	Sharepoint server
MS07-058	933729	Important	Oct 10, 2007	●	●	✗	✗	

MS07-057	939653	Critical	Oct 10, 2007	✓	✓	✗	✗	Internet Explorer
MS07-056	941202	Critical	Oct 9, 2007	●	●	✗	✗	Outlook Express
MS07-055	923810	Critical	Oct 9, 2007	✓	✓	✗	✗	
MS07-054	942099	Important	Sept 12, 2007	●	●	✗	✗	MSN messenger
MS07-053	939778	Important	Sept 12, 2007	●	●	✗	✗	UNIX services
MS07-052	941522	Important	Sept 12, 2007	●	●	✗	✗	Visual Studio
MS07-051	938827	Critical	Sept 12, 2007	✓	✓	✗	✗	Windows 2000
MS07-050	938127	Critical	Aug 14, 2007	✓	✓	✗	✗	Internet Explorer
MS07-049	937986	Important	Aug 14, 2007	●	●	✗	✗	MS Virtual PC
MS07-048	938123	Important	Aug 14, 2007	●	●	✗	✗	MS Vista
MS07-047	936782	Important	Aug 14, 2007	✓	✓	✗	✗	Media Player
MS07-046	938829	Critical	Aug 14, 2007	✓	✓	✗	✗	
MS07-045	937143	Critical	Aug 14, 2007	✓	✓	✗	✗	Internet Explorer
MS07-044	940965	Critical	Aug 14, 2007	✓	✓	✗	✗	Office 2000
MS07-043	921503	Critical	Aug 14, 2007	✓	✓	✗	✗	
MS07-042	936227	Critical	Aug 14, 2007	✓	✓	✗	✗	
MS07-041	939373	Important	July 10, 2007	●	●	✗	✗	IIS 5.1
MS07-040	931212	Critical	July 10, 2007	✓	✓	✗	✗	.Net framework

MS07-039	926122	Critical	July 10, 2007	✓	✓	✗	✗	Windows server
MS07-038	935807	Moderate	July 10, 2007	●	●	✗	✗	MS Vista Firewall
MS07-037	936548	Important	July 10, 2007	●	●	✗	✗	MS Office 2007
MS07-036	936542	Critical	July 10, 2007	✓	✓	✗	✗	MS Excel
MS07-035	935839	Critical	June 12, 2007	✓	✓	✗	✗	
MS07-034	929123	Critical	June 12, 2007	✓	✓	✗	✗	Outlook Express on Windows XP
MS07-033	933566	Critical	June 12, 2007	✓	✓	✗	✗	
MS07-032	931213	Moderate	June 12, 2007	●	●	✗	✗	MS Vista
MS07-031	935840	Critical	June 12, 2007	✓	✓	✗	✗	
MS07-030	927051	Important	June 12, 2007	●	●	✗	✗	MS Visio
MS07-029	935966	Critical	May 8, 2007	✓	✓	✗	✗	Windows servers
MS07-028	931906	Critical	May 8, 2007	●	●	✗	✗	Capicom
MS07-027	931768	Critical	May 8, 2007	✓	✓	✗	✗	Internet Explorer
MS07-026	931832	Critical	May 8, 2007	●	●	✗	✗	Exchange Server
MS07-025	934873	Critical	May 8, 2007	✓	✓	✗	✗	MS Excel
MS07-024	934232	Critical	May 8, 2007	✓	✓	✗	✗	MS Word
MS07-023	934233	Critical	May 8, 2007	✓	✓	✗	✗	MS Excel
MS07-022	931784	Important	Apr 10, 2007	✓	✓	✓	✗	
MS07-021	930178	Critical	Apr 10, 2007	✓	✓	✓	✗	

MS07-020	932168	Critical	Apr 10, 2007	✓	✓	✓	✗	
MS07-019	931261	Critical	Apr 10, 2007	✓	✓	✓	✗	
MS07-018	925939	Critical	Apr 10, 2007	●	●	●	✗	Content Management Server
935448	935448	Important	Apr 20, 2007	✓	✓	✓	✗	
MS07-017	925902	Critical	Apr 03, 2007	!²	!²	!²	✗	935448
MS07-016	928090	Critical	Feb 13, 2007	✓	✓	✓	✗	Internet Explorer
MS07-015	932554	Critical	Feb 13, 2007	✗	✗	✗	✗	MS Access 2000
MS07-014	929434	Critical	Feb 13, 2007	✓	✓	✓	✗	MS Word
MS07-013	918118	Important	Feb 13, 2007	✓	✓	✓	✗	
MS07-012	924667	Important	Feb 13, 2007	✓	✓	✓	✗	
MS07-011	926436	Important	Feb 13, 2007	✓	✓	✓	✗	
MS07-010	932135	Critical	Feb 13, 2007	●	●	●	✗	Malware protection engine
MS07-009	927779	Critical	Feb 13, 2007	✓	✓	!¹	✗	MDAC 2.8
MS07-008	928843	Critical	Feb 13, 2007	!²	!²	!²	✗	935448
MS07-007	927802	Important	Feb 13, 2007	✓	✓	✓	✗	
MS07-006	928255	Important	Feb 13, 2007	✓	✓	✓	✗	
MS07-005	923723	Important	Feb 13, 2007	●	●	●	✗	
MS07-004	929969	Critical	Jan 9, 2007	✓	✓	✓	✗	Internet Explorer
MS07-003	925938	Critical	Jan 9, 2007	✓	✓	✓	✗	MS Outlook 2000

MS07-002	92798	Critical	Jan 9, 2007	✓	✓	✓	✗	MS Excel
MS07-001	921585	Important	Jan 9, 2007	●	●	●	✗	Office 2003