

## Oracle and Microsoft Updates for Symphony

*The Symphony Security Bulletin contains a listing of select Microsoft & Oracle patches that are directly related to the Symphony applications and have been tested against the Symphony applications to validate there are no issues or identify any updates that should NOT be installed. The list is not inclusive of ALL Microsoft or Oracle patches. Customers can load other Microsoft & Oracle patches as MICROS does not expect them to affect Symphony. This report is updated monthly for patches released the prior month and YTD cumulative.*

### Oracle Updates

Date	Version & Patch Level	Symphony Version(s)	Results
1/18/12	11.2.0.2 Patch Set 15	1.5 MR4 1.5 MR5 2.2 2.2 MR1 2.3 2.4	No Issues
1/18/12	Oracle has ended premiere support for the 10.2 Product line		

**MICROS Documentation**

*The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.*

12/19/2011	11.2.0.2 Patch Set 12	1.5 MR4 2.2 2.2 MR1 2.3	No Issues
10/21/11	11.2.0.2 Patch Set 12	2.2 2.2 MR1	No Issues
8/22/11	11.2.0.2 Patch Set 9	2.2 2.2 MR1	No Issues
8/22/11	10.2.0.5 Patch Set 11	1.4 MR5 1.5 1.5 MR2 1.5 MR3	No Issues
7/12/11	11.2.0.2 Patch Set 8	2.1 2.2	No Issues
7/12/11	10.2.0.5 Patch Set 10	1.4 MR5 1.5 1.5MR2 2.1 2.2	No Issues
6/15/11	11.2.0.2	2.1 2.2	No Issues
6/15/11	10.2.0.5 Patch Set 4	1.4 MR5 1.5 1.5MR2 2.1 2.2	No Issues
6/15/11	10.2.0.4 Patch 4	1.4 MR5 1.5 1.5MR2	No Issues

**MICROS Documentation**

*The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.*

		2.1 2.2	
5/26/11	10.2.0.4 Patch 3	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
5/26/11	11.2.0.1 No Patch	2.1 2.2	No Issues

### Microsoft SQL Updates

Date	Version & Patch Level	Simphony Version(s)	Results
1/12/12	SQL Server 2005 SP4	<ul style="list-style-type: none"> <li>1.5 and all inclusive Maintenance Releases</li> <li>2.2 and all inclusive Maintenance Releases</li> <li>2.3</li> <li>2.4</li> </ul>	No Issues
10/11/11 (updated 1/12/12)	SQL Server 2008 SP3	<ul style="list-style-type: none"> <li>1.5 and all inclusive Maintenance Releases</li> <li>2.2 and all inclusive Maintenance Release</li> <li>2.3</li> <li>2.4</li> </ul>	No Issues
7/11/11 (Updated 1/12/12)	SQL Server 2008 R2 SP1	<ul style="list-style-type: none"> <li>1.5 and all inclusive Maintenance Releases</li> <li>2.2 and all inclusive</li> </ul>	No Issues

**MICROS Documentation**

*The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.*

		<b>Maintenance Release</b> <ul style="list-style-type: none"><li>• 2.3</li><li>• 2.4</li></ul>	
--	--	--	--

**MICROS Documentation**

*The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.*

## Microsoft OS Updates

Date	Bulletin Description	Severity	Affected Software	Simphony Version(s)	Results
3/15/12	<a href="#">Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387): MS12-020</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 MR3 1.5 MR4 1.5 MR5 2.2 MR1 2.3 2.4 2.4 MR1	No Issues
3/15/12	<a href="#">Vulnerability in DNS Server Could Allow Denial of Service (2647170): MS12-017</a>	Important	Server 2003 SP2 Server 2008 Server 2008R2	1.5 MR3 1.5 MR4 1.5 MR5 2.2 MR1 2.3 2.4 2.4 MR1	No Issues
3/15/12	<a href="#">Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2641653): MS12-108</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 MR3 1.5 MR4 1.5 MR5 2.2 MR1 2.3 2.4 2.4 MR1	No Issues

### MICROS Documentation

The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.

3/15/12	<a href="#">Vulnerability in DirectWrite Could Allow Denial of Service (2665364): MS12-019</a>	Moderate	Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 MR3 1.5 MR4 1.5 MR5 2.2 MR1 2.3 2.4 2.4 MR1	No Issues
2/15/12	<a href="#">Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465): MS12-008</a>	Critical	<u>Windows XP SP3</u> <u>Windows Vista</u> <u>Windows 7</u> <u>Server 2003 SP2</u> Server 2008 <u>Server 2008R2</u>	<u>1.5 MR3</u> 1.5 MR4 1.5 MR5 <u>2.2</u> 2.2 MR1 2.3 2.4	No Issues
2/15/12	<a href="#">Cumulative Security Update for Internet Explorer (2647516): MS12-010</a>	Critical	<u>Windows XP SP3</u> <u>Windows Vista</u> <u>Windows 7</u> <u>Server 2003 SP2</u> Server 2008 <u>Server 2008R2</u>	<u>1.5 MR3</u> 1.5 MR4 1.5 MR5 <u>2.2</u> 2.2 MR1 2.3 2.4	No Issues
2/15/12	<a href="#">Vulnerability in C Run-Time Library Could Allow Remote Code Execution (2654428): MS12-013</a>	Critical	<u>Windows Vista</u> <u>Windows 7</u> <u>Server 2003 SP2</u> Server 2008 <u>Server 2008R2</u>	<u>1.5 MR3</u> 1.5 MR4 1.5 MR5 <u>2.2</u> 2.2 MR1 2.3 2.4	No issues

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

**MICROS Documentation**

The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.

2/15/12	<a href="#">Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026): MS12-016</a>	Critical	<a href="#">Windows XP SP3</a> <a href="#">Windows Vista</a> <a href="#">Windows 7</a> <a href="#">Server 2003 SP2</a> Server 2008 <a href="#">Server 2008R2</a>	<a href="#">1.5 MR3</a> <b>1.5 MR4</b> <a href="#">1.5 MR5</a> <b>2.2</b> <b>2.2 MR1</b> 2.3 2.4	No Issues
2/15/12	<a href="#">Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640): MS12-009</a>	Important	<a href="#">Windows XP x64 SP2</a> <a href="#">Windows Vista x64 SP2</a> <a href="#">Windows 7</a> <a href="#">Server 2003 SP2</a> Server 2008 x64 SP2 <a href="#">Server 2008R2</a>	<a href="#">1.5 MR3</a> <b>1.5 MR4</b> <a href="#">1.5 MR5</a> <b>2.2</b> <b>2.2 MR1</b> 2.3 2.4	No Issues
2/15/12	<a href="#">Vulnerability in Color Control Panel Could Allow Remote Code Execution (2643719): MS12-012</a>	Important	Server 2008 <a href="#">Server 2008R2</a>	<a href="#">1.5 MR3</a> <b>1.5 MR4</b> <a href="#">1.5 MR5</a> <b>2.2</b> <b>2.2 MR1</b> 2.3 2.4	No Issues
2/15/12	<a href="#">Vulnerability in Indeo Codec Could Allow Remote Code Execution (2661637): MS12-014</a>	Important	<a href="#">Windows XP SP3</a>	<a href="#">1.5 MR3</a> <b>1.5 MR4</b> <a href="#">1.5 MR5</a> <b>2.2</b> <b>2.2 MR1</b> 2.3 2.4	No Issues

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

**MICROS Documentation**

The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.

2/3/12	<a href="#">Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420): MS11-100</a>	Critical	<a href="#">Windows XP SP3</a> <a href="#">Windows Vista</a> <a href="#">Windows 7</a> <a href="#">Server 2003 SP2</a> Server 2008 <a href="#">Server 2008R2</a>	<a href="#">1.5 MR3</a> <a href="#">1.5 MR4</a> <a href="#">1.5 MR5</a> <a href="#">2.2</a> <a href="#">2.2 MR1</a> <a href="#">2.3</a> <a href="#">2.4</a>	No Issues
1/10/12	<a href="#">Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391): MS12-004</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3 2.4	No Issues
1/10/12	<a href="#">Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615): MS12-001</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3 2.4	No Issues
1/10/12	<a href="#">Vulnerability in Windows Object Packager Could Allow Remote Code Execution (2603381): MS12-002</a>	Important	Windows XP SP3 Server 2003 SP2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3 2.4	No Issues

Formatted: Space After: 0 pt, Line spacing: single

Formatted: Space After: 0 pt, Line spacing: single

**MICROS Documentation**

The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.

1/10/12	<a href="#">Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2646524): MS12-003</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3 2.4	No Issues
1/10/12	<a href="#">Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146): MS12-005</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3 2.4	No Issues
1/10/12	<a href="#">Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584): MS12-006</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3 2.4	No Issues
12/19/11	<a href="#">Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417): MS11-087</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues

**MICROS Documentation**

*The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.*

12/19/11	<a href="#">Cumulative Security Update of ActiveX Kill Bits (2618451): MS11-090</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues
12/19/11	<a href="#">Vulnerability in Windows Media Could Allow Remote Code Execution (2648048): MS11-092</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues
12/19/11	<a href="#">Vulnerability in OLE Could Allow Remote Code Execution (2624667): MS11-093</a>	Important	Windows XP SP3 Server 2003 SP2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues
12/19/11	<a href="#">Vulnerability in Active Directory Could Allow Remote Code Execution (2640045): MS11-095</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues

**MICROS Documentation**

*The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.*

12/19/11	<a href="#">Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2620712): MS11-097</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues
12/19/11	<a href="#">Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2633171): MS11-098</a>	Important	Windows XP SP3 Server 2003 SP2 Windows Vista Windows 7 Server 2008	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues
12/19/11	<a href="#">Cumulative Security Update for Internet Explorer (2618444): MS11-099</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues
11/15/11	<a href="#">Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516): MS11-083</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues

**MICROS Documentation**

*The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.*

11/15/11	<a href="#">Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution (2620704): MS11-085</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues
11/15/11	<a href="#">Vulnerability in Active Directory Could Allow Elevation of Privilege (2630837): MS11-086</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues
11/15/11	<a href="#">Vulnerability in Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657)</a>	Moderate	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1 2.3	No Issues
10/11/11	<a href="#">Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2604930): MS11-78</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1	No Issues
10/11/11	<a href="#">Cumulative Security Update for Internet Explorer (2586448): MS11-81</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008	1.5 1.5 MR2 1.5 MR3 1.5 MR4	No Issues

**MICROS Documentation**

*The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.*

			Server 2008R2	2.2 2.2 MR1	
10/11/11	<a href="#">Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (2623699): MS11-75</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1	No Issues
10/11/11	<a href="#">Vulnerability in Windows Media Center Could Allow Remote Code Execution (2604926): MS11-76</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1	No Issues
10/11/11	<a href="#">Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053): MS11-77</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1	No Issues
10/11/11	<a href="#">Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2592799): MS11-80</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.5 1.5 MR2 1.5 MR3 1.5 MR4 2.2 2.2 MR1	No Issues
9/13/11	<a href="#">Vulnerability in WINS Could Allow Elevation of Privilege (2571621): MS11-70</a>	Important	Server 2003 SP2 Server 2008 Server 2008 R2	1.4 MR5 1.5 1.5 MR2 1.5 MR3 2.2	No Issues

**MICROS Documentation**

The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.

				2.2 MR1	
9/13/11	<a href="#">Vulnerability in Windows Components Could Allow Remote Code Execution (2570947): MS11-71</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 1.5 MR3 2.2 2.2 MR1	No Issues
8/11/11	<a href="#">Cumulative Security Update for Internet Explorer (2559049): MS11-057</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 1.5 MR3 2.2 2.2 MR1	No Issues
8/11/11	<a href="#">Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485): MS11-058</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 SP2 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 1.5 MR3 2.2 2.2 MR1	No Issues
8/11/11	<a href="#">Vulnerability in Data Access Components Could Allow Remote Code Execution (2560656): MS11-059</a>	Important	Windows 7 Windows 7 SP1 Server 2008R2 Server 2008R2 SP1	1.4 MR5 1.5 1.5 MR2 1.5 MR3 2.2 2.2 MR1	No Issues
8/11/11	<a href="#">Vulnerability in Remote Desktop Web Access Could Allow Elevation of Privilege (2546250): MS 11-061</a>	Important	Server 2008R2 Server 2008R2 SP1	1.5 MR3 2.2 2.2 MR1	No Issues
8/11/11	<a href="#">Vulnerability in Remote Access Service NDISTAPI Driver Could Allow Elevation of Privilege (2566454): MS11-062</a>	Important	Windows XP SP3 Server 2003 SP2	1.4 MR5 1.5 1.5 MR2	No Issues

**MICROS Documentation**

The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.

				1.5 MR3 2.2 2.2 MR1	
8/11/11	<a href="#">Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680): MS11-063</a>	Important	Windows XP SP3 Windows Vista SP2 Windows 7 Windows 7 SP1 Server 2003 SP2 Server 2008 Server 2008R2 Server 2008R2 SP1	1.4 MR5 1.5 1.5 MR2 1.5 MR3 2.2 2.2 MR1	No Issues
8/11/11	<a href="#">Vulnerabilities in TCP/IP Stack Could Allow Denial of Service (2563894): MS11-064</a>	Important	Windows Vista SP2 Windows 7 Windows 7 SP1 Server 2008 Server 2008R2 Server 2008R2 SP1	1.4 MR5 1.5 1.5 MR2 1.5 MR3 2.2 2.2 MR1	No Issues
8/11/11	<a href="#">Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (2570222): MS11-065</a>	Important	Windows XP SP3 Server 2003 SP2	1.4 MR5 1.5 1.5 MR2 1.5 MR3 2.2 2.2 MR1	No Issues
8/11/11	<a href="#">Vulnerability in Windows Kernel Could Allow Denial of Service (2556532): MS11-068</a>	Moderate	Windows Vista SP2 Windows 7 Windows 7 SP1 Server 2008 Server 2008R2 Server 2008R2 SP1	1.4 MR5 1.5 1.5 MR2 1.5 MR3 2.2 2.2 MR1	No Issues
8/11/11	<a href="#">Vulnerability in .NET Framework Could Allow Information Disclosure (2567951): MS11-069</a>	Moderate	Windows XP SP3 Windows Vista SP2 Windows 7	1.4 MR5 1.5 1.5 MR2	No Issues

**MICROS Documentation**

The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.

			Windows 7 SP1 Server 2003 SP2 Server 2008 Server 2008R2 Server 2008R2 SP1	1.5 MR3 2.2 2.2 MR1	
8/11/11	<a href="#">MSSQL SQL Server 2008 R2 SP1</a>	Important	Server 2008 Server 2008R2 Server 2008R2 SP1	1.5 MR3 2.2 2.2 MR1	No Issues
7/12/11	<a href="#">Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2507938): MS11-056</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
7/12/11	<a href="#">Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917): MS11-054</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
7/12/11	<a href="#">Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (2566220): MS11-053</a>	Critical	Windows Vista Windows 7	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
7/12/11	<a href="#">Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2544521): MS11-052</a>	Critical	IE6, IE7, IE8 in Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
6/15/11	<a href="#">Vulnerability in Active Directory</a>	Important	Windows XP SP3 Windows Vista	1.4 MR5	No Issues

**MICROS Documentation**

The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.

	<a href="#">Certificate Services Web Enrollment Could Allow Elevation of Privilege (2518295): MS11-051</a>		Windows 7 Server 2003 Server 2008 Server 2008R2	1.5 1.5 MR2 2.1 2.2	
6/15/11	<a href="#">Vulnerability in SMB Server Could Allow Denial of Service (2536275): MS11-048</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
6/15/11	<a href="#">Vulnerability in Hyper-V Could Allow Denial of Service (2525835): MS11-047</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
6/15/11	<a href="#">Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2503665): MS11-046</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
6/15/11	<a href="#">Vulnerability in MHTML Could Allow Information Disclosure (2544893): MS11-037</a>	Important	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
6/15/11	<a href="#">Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2544521): MS11-052</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues

**MICROS Documentation**

*The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.*

6/15/11	<a href="#">Cumulative Security Update for Internet Explorer (2530548): MS11-050</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
6/15/11	<a href="#">Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814): MS11-044</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
6/15/11	<a href="#">Vulnerability in SMB Client Could Allow Remote Code Execution (2536276): MS11-043</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
6/15/11	<a href="#">Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2525694): MS11-041</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
6/15/11	<a href="#">Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842): MS11-039</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003 Server 2008 Server 2008R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
6/15/11	<a href="#">Vulnerability in OLE Automation Could Allow Remote Code Execution (2476490): MS11-038</a>	Critical	Windows XP SP3 Windows Vista Windows 7 Server 2003	1.4 MR5 1.5 1.5 MR2 2.1	No Issues

**MICROS Documentation**

The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.

			Server 2008 Server 2008R2	2.2	
6/15/11	<a href="#">Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure (2543893): MS11-049</a>	Important	SQL Server 2005 SQL Server 2008 SQL Server 2008 R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
6/15/11	<a href="#">Vulnerabilities in Distributed File System Could Allow Remote Code Execution (2535512): MS11-042</a>	Critical	Server 2003 XP Vista Windows 7 Server 2008 Server 2008 R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues
5/26/11	<a href="#">Vulnerability in WINS Could Allow Remote Code Execution (2524426): MS11-035</a>	Critical	Server 2003 XP Vista Windows 7 Server 2008 Server 2008 R2	1.4 MR5 1.5 1.5 MR2 2.1 2.2	No Issues

**MICROS Documentation**

*The information contained herein reflects MICROS Systems test results in respect to Microsoft's Security Bulletins. This document does not bind MICROS Systems Inc., to any contractual obligations. Please refer to Section 8 of the Standard Terms & Conditions on the MICROS sales contract.*