

Microsoft Security Bulletins for

Application Server Platforms

Windows 2000 Opera V4.0.5+
 Windows 2003 (32 Bit) Opera V4.0.5+
 Windows 2003 (x64 Bit) Opera V4.0.5+ and v5.0+

Database Server Platforms

Windows 2000 Opera V4.0.5+
 Windows 2003 (32/64 Bit) Opera V2.0.5+
 Windows 2003 (X64 Bit) Opera V4.0.5+ and v5.0+
 Windows 2008 (x64 bit) Opera V5.0.1.03 e3+

Date	Bulletin Description	Severity	Results
May 11, 2012	Vulnerability in Windows Partition Manager Could Allow Elevation of Privilege (2690533) MS12-033	Important	No issues
May 11, 2012	Vulnerability in TCP/IP Could Allow Elevation of Privilege (2688338) MS12-032	Important	No issues
May 11, 2012	Vulnerability in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2597981) MS12-031	Important	No issues
May 11, 2012	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2663830) MS12-030	Important	No issues
May 11, 2012	Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777) MS12-035	Critical	No issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
May 11, 2012	Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578) MS12-034	Critical	No Issues
May 11, 2012	Vulnerability in Microsoft Word Could Allow Remote Code Execution (2680352) MS12-029	Critical	No Issues
April 12, 2012	Vulnerability in Microsoft Office Could Allow Remote Code Execution (2639185) MS12-028	Important	No Issues
April 12, 2012	Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Information Disclosure (2663860) MS12-026	Important	No Issues
April 12, 2012	Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2664258) MS12-027	Critical	No Issues
April 12, 2012	Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605) MS12-025	Critical	No Issues
April 12, 2012	Vulnerability in Windows Could Allow Remote Code Execution (2653956) MS12-024	Critical	No Issues
April 12, 2012	Cumulative Security Update for Internet Explorer (2675157) MS12-023	Critical	No Issues
March 13, 2012	Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) MS12-020	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
March 13, 2012	Vulnerability in DNS Server Could Allow Denial of Service (2647170) MS12-017	Important	No Issues
March 13, 2012	Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2641653) MS12-018	Important	No Issues
March 13, 2012	Vulnerability in Visual Studio Could Allow Elevation of Privilege (2651019) MS12-021	Important	No Issues
March 13, 2012	Vulnerability in Expression Design Could Allow Remote Code Execution (2651018) MS12-022	Important	No Issues
March 13, 2012	Vulnerability in DirectWrite Could Allow Denial of Service (2665364) MS12-019	Moderate	No Issues
February 14, 2012	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465) MS12-008	Critical	No Issues
February 14, 2012	Cumulative Security Update for Internet Explorer (2647516) MS12-010	Critical	No Issues
February 14, 2012	Vulnerability in C Run-Time Library Could Allow Remote Code Execution (2654428) MS12-013	Critical	No Issues
February 14, 2012	Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026) MS12-016	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
February 14, 2012	Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640) MS12-009	Important	No Issues
February 14, 2012	Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2663841) MS12-011	Important	No Issues
February 14, 2012	Vulnerability in Color Control Panel Could Allow Remote Code Execution (2643719) MS12-012	Important	No Issues
February 14, 2012	Vulnerability in Indeo Codec Could Allow Remote Code Execution (2661637) MS12-014	Important	No Issues
February 14, 2012	Vulnerabilities in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2663510) MS12-015	Important	No Issues
January 10, 2012	Vulnerability in AntiXSS Library Could Allow Information Disclosure (2607664) MS12-007	Important	No Issues
January 10, 2012	Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584) MS12-006	Important	No Issues
January 10, 2012	Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146) MS12-005	Important	No Issues
January 10, 2012	Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391) MS12-004	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
January 10, 2012	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2646524) MS12-003	Important	No Issues
January 10, 2012	Vulnerability in Windows Object Packager Could Allow Remote Code Execution (2603381) MS12-002	Important	No Issues
January 10, 2012	Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615) MS12-001	Important	No Issues
December 13, 2011	Cumulative Security Update for Internet Explorer (2618444) MS11-099	Important	No issues
December 13, 2011	Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2633171) MS11-098	Important	No Issues
December 13, 2011	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2620712) MS11-097	Important	No Issues
December 13, 2011	Vulnerability in Microsoft Excel Could Allow Remote Code Execution (2640241) MS11-096	Important	No Issues
December 13, 2011	Vulnerability in Active Directory Could Allow Remote Code Execution (2640045) MS11-095	Important	No Issues
December 13, 2011	Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2639142) MS11-094	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
December 13, 2011	Vulnerability in OLE Could Allow Remote Code Execution (2624667) MS11-093	Important	No Issues
December 13, 2011	Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2607702) MS11-091	Important	No Issues
December 13, 2011	Vulnerability in Microsoft Office Could Allow Remote Code Execution (2590602) MS11-089	Important	No Issues
December 13, 2011	Vulnerability in Microsoft Office IME (Chinese) Could Allow Elevation of Privilege (2652016) MS11-088	Important	No Issues
December 13, 2011	Vulnerability in Windows Media Could Allow Remote Code Execution (2648048) MS11-092	Critical	No Issues
December 13, 2011	Cumulative Security Update of ActiveX Kill Bits (2618451) MS11-090	Critical	No Issues
December 13, 2011	Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417) MS11-087	Critical	No Issues
November 8, 2011	Vulnerability in Active Directory Could Allow Elevation of Privilege (2630837) MS11-086	Important	No Issues
November 8, 2011	Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution (2620704) MS11-085	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
November 8, 2011	Vulnerability in Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657) MS11-084	Moderate	No Issues
November 8, 2011	Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516) MS11-083	Critical	No Issues
October 11, 2011	Vulnerabilities in Host Integration Server Could Allow Denial of Service (2607670) MS11-082	Important	No Issues
October 11, 2011	Cumulative Security Update for Internet Explorer (2586448) MS11-081	Critical	No Issues
October 11, 2011	Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2592799) MS11-080	Important	No Issues
October 11, 2011	Vulnerabilities in Microsoft Forefront Unified Access Gateway Could Cause Remote Code Execution (2544641) MS11-079	Important	No Issues
October 11, 2011	Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2604930) MS11-078	Critical	No Issues
October 11, 2011	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053) MS11-077	Important	No Issues
October 11, 2011	Vulnerability in Windows Media Center Could Allow Remote Code Execution (2604926) MS11-076	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
October 11, 2011	Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (2623699) MS11-075	Important	No Issues
September 13, 2011	Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2451858) MS11-074	Important	No Issues
September 13, 2011	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2587634) MS11-073	Important	No Issues
September 13, 2011	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2587505) MS11-072	Important	No Issues
September 13, 2011	Vulnerability in Windows Components Could Allow Remote Code Execution (2570947) MS11-071	Important	No Issues
September 13, 2011	Vulnerability in WINS Could Allow Elevation of Privilege (2571621) MS11-070	Important	No Issues
August 9, 2011	Vulnerability in .NET Framework Could Allow Information Disclosure (2567951) MS11-069	Important	No Issues
August 9, 2011	Vulnerability in Windows Kernel Could Allow Denial of Service (2556532) MS11-068	Important	No Issues
August 9, 2011	Vulnerability in Microsoft Report Viewer Could Allow Information Disclosure (2578230) MS11-067	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
August 9, 2011	Vulnerability in Microsoft Chart Control Could Allow Information Disclosure (2567943) MS11-066	Important	No Issues
August 9, 2011	Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (2570222) MS11-065	Important	No issues
August 9, 2011	Vulnerabilities in TCP/IP Stack Could Allow Denial of Service (2563894) MS11-064	Important	No Issues
August 9, 2011	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680) MS11-063	Important	No Issues
August 9, 2011	Vulnerability in Remote Access Service NDISTAPI Driver Could Allow Elevation of Privilege (2566454) MS11-062	Important	No Issues
August 9, 2011	Vulnerability in Remote Desktop Web Access Could Allow Elevation of Privilege (2546250) MS11-061	Important	No Issues
August 9, 2011	Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (2560978) MS11-060	Important	No Issues
August 9, 2011	Vulnerability in Data Access Components Could Allow Remote Code Execution (2560656) MS11-059	Important	No Issues
August 9, 2011	Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) MS11-058	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
August 9, 2011	Cumulative Security Update for Internet Explorer (2559049) MS11-057	Critical	No Issues
July 12,2011	Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2507938) MS11-056	Important	No Issues
July 12, 2011	Vulnerability in Microsoft Visio Could Allow Remote Code Execution (2560847) MS11-055	Important	No Issues
July 12, 2011	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917) MS11-054	Important	No Issues
July 12, 2011	Vulnerability in Bluetooth Stack Could Allow Remote Code Execution (2566220) MS11-053	Critical	No Issues
June 16, 2011	Vulnerability in MHTML Could Allow Information Disclosure (2544893) MS11-037	Important	No Issues
June 16, 2011	Vulnerability in OLE Automation Could Allow Remote Code Execution (2476490) MS11-038	Critical	No Issues
June 16, 2011	Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2514842) MS11-039	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
June 16, 2011	Security update for the .NET Framework 3.5 Service Pack 1 and .NET Framework 2.0 Service Pack 2 on Windows XP Service Pack 3 and on Windows Server 2003 Service Pack 2: June 14, 2011 (2478658) MS11-039	Critical	No Issues
June 16, 2011	Security update for the .NET Framework 4 on Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2: June 14, 2011 (2478663) MS11-039	Critical	No Issues
June 16, 2011	Security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and on Windows Server 2008 R2 Service Pack 1: June 14, 2011 (2478662) MS11-039	Critical	No Issues
June 16, 2011	Security update for the .NET Framework 3.5 Service Pack 1, Windows Vista Service Pack 2 and Windows Server 2008 Service Pack 2: June 14, 2011 (2478660) MS11-039	Critical	No Issues
June 16, 2011	Vulnerability in Threat Management Gateway Firewall Client Could Allow Remote Code Execution (2520426) MS11-040	Critical	No Issues
June 16, 2011	Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2525694) MS11-041	Critical	No Issues
June 16, 2011	Vulnerabilities in Distributed File System Could Allow Remote Code Execution (2535512) MS11-042	Critical	No Issues
June 16, 2011	Vulnerability in SMB Client Could Allow Remote Code Execution (2536276) MS11-043	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
June 16, 2011	Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814) MS11-044	Critical	No Issues
June 16, 2011	Security update for the .NET Framework 4 on Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2: June 14, 2011 (2518870) MS11-044	Critical	No Issues
June 16, 2011	Security update for the .NET Framework 3.5 Service Pack 1 and .NET Framework 2.0 Service Pack 2 on Windows XP Service Pack 3 and on Windows Server 2003 Service Pack 2: June 14, 2011 (2518864) MS11-044	Critical	No Issues
June 16, 2011	Security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and on Windows Server 2008 R2 Service Pack 1: June 14, 2011 (2518869) MS11-044	Critical	No Issues
June 16, 2011	Security update for the .NET Framework 3.5 Service Pack 1, Windows Vista Service Pack 2 and Windows Server 2008 Service Pack 2: June 14, 2011 (2518866) MS11-044	Critical	No Issues
June 16, 2011	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2537146) MS11-045	Important	No Issues
June 16, 2011	Security update for the Excel 2007 converter: June 14, 2011 (2541012) MS11-045	Important	No Issues
June 16, 2011	Security update for Excel 2007: June 14, 2011 (2541007) MS11-045	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
June 16, 2011	Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2503665) MS11-046	Important	No Issues
June 16, 2011	Vulnerability in Hyper-V Could Allow Denial of Service (2525835) MS11-047	Important	No Issues
June 16, 2011	Vulnerability in SMB Server Could Allow Denial of Service (2536275) MS11-048	Important	No Issues
June 16, 2011	Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure (2543893) MS11-049	Important	No Issues
June 16, 2011	Security update for InfoPath 2007: June 14, 2011 (2510061) MS11-049	Important	No Issues
June 16, 2011	Cumulative Security Update for Internet Explorer (2530548) MS11-050	Critical	No Issues
June 16, 2011	Vulnerability in Active Directory Certificate Services Web Enrollment Could Allow Elevation of Privilege (2518295) MS11-051	Important	No Issues
June 16, 2011	Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2544521) MS11-052	Critical	No Issues
May 20, 2011	Vulnerability in WINS Could Allow Remote Code Execution (2524426) MS11-035	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
May 20, 2011	Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2545814) MS11-036	Important	No Issues
May 20, 2011	Description of the security update for PowerPoint 2003: May 10, 2011 (2535812) MS11-036	Important	No issues
May 20, 2011	Description of the security update for PowerPoint 2007: May 10, 2011 (2535818) MS11-036	Important	No Issues
April 19, 2011	Cumulative Security Update for Internet Explorer (2497640) MS11-018	Critical	No Issues
April 19, 2011	Vulnerabilities in SMB Client could allow remote code execution: April 12, 2011 (2511455) MS11-019	Critical	No Issues
April 19, 2011	Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) MS11-020	Critical	No Issues
April 19, 2011	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2489279) MS11-021	Important	No Issues
April 19, 2011	Security update for the 2007 Office system and the Office Compatibility Pack: April 12, 2011 (2466156) MS11-021	Important	No Issues
April 19, 2011	Security update for Excel 2007: April 12, 2011 (2464583) MS11-021	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
April 19, 2011	Security update for Excel 2003: April 12, 2011 (2502786) MS11-021	Important	No issues
April 19, 2011	Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2489283) MS11-022	Important	No Issues
April 19, 2011	Security update for PowerPoint 2007: April 12, 2011 (2464594) MS11-022	Important	No Issues
April 19, 2011	Security update for PowerPoint Viewer 2007: April 12, 2011 (2464623) MS11-022	Important	No issues
April 19, 2011	Security update for PowerPoint 2003: April 12, 2011 (2464588) MS11-022	Important	No Issues
April 19, 2011	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2489293) MS11-023	Important	No Issues
April 19, 2011	Security update for 2007 Office system: April 12, 2011 (2509488) MS11-023	Important	No Issues
April 19, 2011	Security update for Office 2003: April 12, 2011 (2509503) MS11-023	Important	No issues
April 19, 2011	Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution (2527308) MS11-024	Important	No issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
April 19, 2011	Security update for Windows Fax Cover Page Editor MFC components: April 12, 2011 (2506212) MS11-024	Important	No Issues
April 19, 2011	Security update for the JScript and VBScript v5.7 scripting engines: April 12, 2011 (2491683) MS11-024	Important	No Issues
April 19, 2011	Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212) MS11-025	Important	No Issues
April 19, 2011	Security update for Visual C++ 2005 SP1 Redistributable Package: April 12, 2011 (2467175) MS11-025	Important	No Issues
April 19, 2011	Vulnerability in MHTML Could Allow Information Disclosure (2503658) MS11-026	Important	No Issues
April 19, 2011	Cumulative Security Update of ActiveX Kill Bits (2508272) MS11-027	Critical	No Issues
April 19, 2011	Vulnerability in .NET Framework Could Allow Remote Code Execution (2484015) MS11-028	Critical	No Issues
April 19, 2011	Security update for the .NET Framework 3.5 Service Pack 1 and the .NET Framework 2.0 Service Pack 2 on Windows Server 2003 and Windows XP: April 12, 2011 (2446704) MS11-028	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
April 19, 2011	Security update for the .NET Framework 4 on Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2: April 12, 2011 (2446708) MS11-028	Critical	No Issues
April 19, 2011	Security update for the .NET Framework 3.5 Service Pack 1 and the .NET Framework 2.0 Service Pack 2 on Windows Vista Service Pack 2 and Windows Server 2008 Service Pack 2: April 12, 2011 (2449742) MS11-028	Critical	No Issues
April 19, 2011	Security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and on Windows Server 2008 R2 Service Pack 1: April 12, 2011 (2446710) MS11-028	Critical	No Issues
April 19, 2011	Vulnerability in GDI+ Could Allow Remote Code Execution (2489979) MS11-029	Critical	No Issues
April 19, 2011	Security update for Windows GDI+: April 12, 2011 (2412687) MS11-029	Critical	No Issues
April 19, 2011	Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) MS11-030	Critical	No Issues
April 19, 2011	Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2514666) MS11-031	Critical	No Issues
April 19, 2011	Security update for the JScript and VBScript v5.8 scripting engines: April 12, 2011 (2510531) MS11-031	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
April 19, 2011	Security update for the JScript and VBScript v5.7 scripting engines: April 12, 2011 (2510581) MS11-031	Critical	No Issues
April 19, 2011	Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2507618) MS11-032	Critical	No Issues
April 19, 2011	Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2485663) MS11-033	Critical	No Issues
April 19, 2011	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2506223) MS11-034	Critical	No Issues
April 19, 2011	Microsoft Security Advisory: Fraudulent Digital Certificates could allow spoofing (2524375)	Critical	No Issues
April 19, 2011	Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution (2510587) MS11-031	Critical	No Issues
Mar 15, 2011	Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030) MS11-015	Critical	No Issues
Mar 15, 2011	Description of the security update for Microsoft Windows: March 8, 2011 (2479943) MS11-015	Critical	No Issues
Mar 15, 2011	Vulnerability in Microsoft Groove Could Allow Remote Code Execution (2494047) MS11-016	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Mar 15, 2011	Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2508062) MS11-017	Important	No Issues
Mar 15, 2011	Description of the security update for Remote Desktop client 6.1 and Remote Desktop client 6.0: March 8, 2011 (2481109) MS11-017	Important	No Issues
Feb 8, 2011	Vulnerability in Local Security Authority Subsystem Service Could Allow Local Elevation of Privilege (2478960): MS11-014	Important	No Issues
Feb 8, 2011	Security update for Kerberos in Windows XP and in Windows Server 2003: February 8, 2011 (2478971) MS11-013	Important	No Issues
Feb 8, 2011	Security update for Kerberos in Windows 7 and in Windows Server 2008 R2: February 8, 2011 (2425227) MS11-013	Important	No Issues
Feb 8, 2011	Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930): MS11-013	Important	No Issues
Feb 8, 2011	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628): MS11-012	Important	No Issues
Feb 8, 2011	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802): MS11-011	Important	No issues
Feb 8, 2011	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2476687): MS11-010	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Feb 8, 2011	Vulnerability in JScript and VBScript Scripting Engines Could Allow Information Disclosure (2475792) MS11-009	Important	No Issues
Feb 8, 2011	Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (2451879) MS11-008	Important	No Issues
Feb 8, 2011	Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376) MS11-007	Critical	No issues
Feb 8, 2011	Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185) MS11-006	Critical	No Issues
Feb 8, 2011	Vulnerability in Active Directory Could Allow Denial of Service (2478953) MS11-005	Important	No Issues
Feb 8, 2011	Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256) MS11-004	Important	No Issues
Feb 8, 2011	Cumulative Security Update for Internet Explorer (2416400): MS11-003	Critical	No Issues
Jan 14, 2010	Vulnerability in Windows Backup Manager Could Allow Remote Code Execution (2478935) MS11-001	Important	No Issues
Jan 14, 2010	Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (2451910) MS11-002	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Jan 14, 2010	Security update for Microsoft Data Access Components 2.8 Service Pack 1: January 11, 2011 (2419632) MS11-002	Critical	No Issues
Jan 14, 2010	Security update for Windows Data Access Components 6.0: January 11, 2011 (2419640) MS11-002	Critical	No Issues
Jan 14, 2010	Security update for Microsoft Data Access Components 2.8 Service Pack 2: January 11, 2011 (2419635) MS11-002	Critical	No Issues
Dec 14, 2010	Vulnerabilities in the Open Type Font (OTF) Driver Could Allow Remote Code Execution (2296199) MS10-091	Critical	No Issues
Dec 14, 2010	Vulnerability in Task Scheduler Could Allow Elevation of Privilege (2305420) MS10-092	Critical	No Issues
Dec 14, 2010	Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (2424434) MS10-093	Critical	No Issues
Dec 14, 2010	Vulnerability in Windows Media Encoder Could Allow Remote Code Execution (2447961) MS10-094	Critical	No Issues
Dec 14, 2010	Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution (2443105) MS10-097	Critical	No Issues
Dec 14, 2010	Vulnerability in Routing and Remote Access Could Allow Elevation of Privilege (2440591) MS10-099	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Dec 14, 2010	Vulnerability in Consent User Interface Could Allow Elevation of Privilege (2442962) MS10-100	Critical	No Issues
Dec 14, 2010	Vulnerability in Windows Net logon Service Could Allow Denial of Service (2207559) MS10-101	Critical	No Issues
Dec 14, 2010	Vulnerability in Hyper-V Could Allow Denial of Service (2345316) MS10-102	Critical	No Issues
Dec 14, 2010	Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2292970) MS10-103	Critical	No Issues
Dec 14, 2010	Description of the security update for Microsoft Office Publisher 2003: December 14, 2010 (2284695) MS10-103	Critical	No Issues
Dec 14, 2010	Description of the security update for Microsoft Office Publisher 2007: December 14, 2010 (2284697) MS10-103	Critical	No Issues
Dec 14, 2010	Vulnerability in Microsoft SharePoint Could Allow Remote Code Execution (2455005) MS10-104	Important	No Issues
Dec 14, 2010	Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095) MS10-105	Important	No Issues
Dec 14, 2010	Description of the security update for the 2007 Microsoft Office system: December 14, 2010 (2288931) MS10-105	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Dec 14, 2010	Description of the security update for Microsoft Office 2003: December 14, 2010 (2289163) MS10-105	Important	No Issues
Dec 14, 2010	Vulnerability in Microsoft Exchange Server Could Allow Denial of Service (2407132) MS10-106	Moderate	No Issues
Dec 14, 2010	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673): MS10-098	Important	No Issues
Dec 14, 2010	Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089) MS10-096	Critical	No Issues
Dec 14, 2010	An update is available for Internet Explorer: December 14, 2010 (2467659)	Important	No Issues
Dec 14, 2010	Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2385678): MS10-095	Important	No Issues
Dec 14, 2010	Cumulative Security Update for Internet Explorer (2416400) MS10-090	Critical	No Issues
Dec 14, 2010	Cumulative Security Update for Internet Explorer (2360131): MS10-090	Critical	No Issues
Oct 12, 2010	Vulnerability in Windows Local Procedure Call Could Cause Elevation of Privilege (2360937): MS10-084	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Oct 12, 2010	Description of the update that implements Extended Protection for Authentication in the Server service (2345886)	Important	No Issues
Oct 12, 2010	Security update for WordPad: October 12, 2010 (979687) MS10-083	Important	No Issues
Oct 12, 2010	Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution (2405882): MS10-083	Important	No Issues
Oct 12, 2010	Vulnerability in Windows Media Player Could Allow Remote Code Execution (2378111) MS10-082	Important	No Issues
Oct 12, 2010	Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2296011): MS10-081	Important	No Issues
Oct 12, 2010	Vulnerabilities in the OpenType Font (OTF) Format Driver Could Allow Elevation of Privilege (2279986) MS10-078	Important	No Issues
Oct 12, 2010	Vulnerability in .NET Framework Could Allow Remote Code Execution (2160841): MS10-077	Critical	No Issues
Oct 12, 2010	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132) MS10-076	Critical	No Issues
Oct 12, 2010	Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution (2387149): MS10-074	Moderate	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Oct 12, 2010	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957): MS10-073	Important	No Issues
Oct 12, 2010	Cumulative Security Update for Internet Explorer (2360131): MS10-071	Critical	No Issues
Sep 14, 2010	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2121546): MS10-069	Important	No Issues
Sep 14, 2010	Vulnerability in Local Security Authority Subsystem Service Could Allow Elevation of Privilege (983539): MS10-068	Important	No Issues
Sep 14, 2010	Vulnerability in Remote Procedure Call Could Allow Remote Code Execution (982802): MS10-066	Important	No Issues
Sep 14, 2010	Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960): MS10-065	Important	No Issues
Sep 14, 2010	Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290): MS10-061	Critical	No Issues
Aug 11, 2010	Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198) MS10-046	Critical	No Issues
Aug 11, 2010	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852) MS10-047	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Aug 11, 2010	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329) MS10-048	Important	No Issues
Aug 11, 2010	Vulnerabilities in SChannel Could Allow Remote Code Execution (980436) MS10-049	Critical	No Issues
Aug 11, 2010	Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (981997) MS10-050	Important	No Issues
Aug 11, 2010	Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2079403) MS10-051	Critical	No issues
Aug 11, 2010	Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (2115168) MS10-052	Critical	No Issues
Aug 11, 2010	Cumulative Security Update for Internet Explorer (2183461) MS10-053	Critical	No Issues
Aug 11, 2010	Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) MS10-054	Critical	No Issues
Aug 11, 2010	Vulnerability in Cinepak Codec Could Allow Remote Code Execution (982665) MS10-055	Critical	No Issues
Aug 11, 2010	Vulnerabilities in Microsoft Office Word could allow remote code execution (2269638) MS10-056	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Aug 11, 2010	Security update for the 2007 Office system and for the Compatibility Pack for the 2007 Office system: August 10, 2010 (2277947) MS10-056	Critical	No Issues
Aug 11, 2010	Security update for Word 2007: August 10, 2010 (2251419) MS10-056	Critical	No Issues
Aug 11, 2010	Security update for Word 2003: August 10, 2010 (2251399) MS10-056	Critical	No Issues
Aug 11, 2010	Vulnerability in Microsoft Office Excel Could Allow Remote Code Execution (2269707) MS10-057	Important	No Issues
Aug 11, 2010	Security update for Excel 2003: August 10, 2010 (2264403) MS10-057	Important	No Issues
Aug 11, 2010	Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886) MS10-058	Important	No Issues
Aug 11, 2010	Vulnerabilities in the Tracing Feature for Services Could Allow an Elevation of Privilege (982799) MS10-059	Important	No Issues
Aug 11, 2010	Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906) MS10-060	Critical	No Issues
Jul 13,2010	Vulnerability in Help and Support Center Could Allow Remote Code Execution (2229593): MS10-042	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Jun 8, 2010	Vulnerability in Microsoft .NET Framework Could Allow Tampering (981343) : MS10-041	Important	No Issues
Jun 8, 2010	Vulnerability in Internet Information Services Could Allow Remote Code Execution (982666) : MS10-040	Important	No Issues
Jun 8, 2010	Vulnerability in COM validation in Microsoft Office Could Allow Remote Code Execution (983235) : MS10-036	Important	No Issues
Jun 8, 2010	Cumulative Security Update for Internet Explorer (982381) : MS10-035	Critical	No Issues
June 8, 2010	Cumulative Security Update for Internet Explorer (982381) : MS10-035	Critical	No Issues
June 8, 2010	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559) : MS10-032	Important	No Issues
Apr 13, 2010	Vulnerability in Windows ISATAP Component Could Allow Spoofing (978338) : MS10-029	Important	No Issues
Apr 13, 2010	Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169) : MS10-022	Important	No Issues
Apr 13, 2010	Vulnerabilities in Windows Kernel could allow Elevation of Privilege (979683) : MS10-021	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Apr 13, 2010	Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232) : MS10-020	Critical	No Issues
Apr 13, 2010	Vulnerabilities in Windows Could Allow Remote Code Execution (981210) : MS10-019	Critical	No Issues
Feb 9, 2010	Vulnerabilities in Windows Kernel could allow Elevation of Privilege (977165) : MS10-015	Important	No Issues
Feb 9, 2010	Vulnerability in Kerberos Could Allow Denial of Service (977290) : MS10-014	Important	No Issues
Feb 9, 2010	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935) : MS10-013	Critical	No Issues
Feb 9, 2010	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468) : MS10-012	Important	No Issues
Feb 9, 2010	Vulnerabilities in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege (978037) : MS10-011	Important	No Issues
Feb 9, 2010	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145) : MS10-009	Critical	No Issues
Feb 9, 2010	Cumulative Security Update of ActiveX Kill Bits (978262) : MS10-008	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Feb 9 ,2010	Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (975713) : MS10-007	Critical	No Issues
Feb 9 ,2010	Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251) : MS10-006	Critical	No Issues
Jan 21, 2010	Critical Cumulative Security Update for Internet Explorer (978207) : MS10-002	Critical	No Issues
Jan 12, 2010	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270) : MS10-001	Critical for Win 2000 Otherwise Low	No Issues
Dec 8, 2009	Cumulative Security Update for Internet Explorer (974455) : MS09-072	Critical	No Issues
Dec 8, 2009	Vulnerability on Internet Authentication Service Could Allow Remote Code Execution (974318) : MS09-071	Critical	No Issues
Dec 8, 2009	Vulnerabilities in Active Directory Federation Services Could Allow Remote Code Execution (971726) : MS09-070	Important	No Issues
Dec 8, 2009	Vulnerability in Local Security Subsystem Authority Service Could Allow Denial of Service (974392) : MS09-069	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Nov 11, 2009	Vulnerability in Active Directory Could Allow Denial of Service (973309) : MS09-066	Important	No Issues
Nov 11, 2009	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947) : MS09-065	Critical	No Issues
October 13, 2009	Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488) : MS09-062	Critical	No Issues
October 13, 2009	Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution (974378) : MS09-061	Critical	No Issues
October 13, 2009	Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (975467) : MS09-059	Important	No Issues
October 13, 2009	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (971486) : MS09-058	Important	No Issues
October 13, 2009	Vulnerability in Indexing Service Could Allow Remote Code Execution (969059) : MS09-057	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
October 13, 2009	Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571) : MS09-056	Important	No Issues
October 13, 2009	Cumulative Security Update of ActiveX Kill Bits (973525) : MS09-055	Critical	No Issues
October 13, 2009	Cumulative Security Update for Internet Explorer (974455) : MS09-054	Critical	No Issues
October 13, 2009	Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517) : MS09-050	Critical	No Issues
Sep 9, 2009	Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution (971961) MS09-045	Critical	No Issues
Sep 9, 2009	Vulnerability in Wireless LAN AutoConfig Service Could Allow Remote Code Execution (970710) MS09-049	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Sep 9, 2009	Vulnerabilities in Windows Media Format Could Allow Remote Code Execution (973812) MS09-047	Critical	No Issues
Sep 9, 2009	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723) MS09-048	Critical	No Issues
Sep 9, 2009	Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (956844) MS09-046	Critical	No Issues
Aug 11, 2009	Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (970927) : MS09-044	Critical	No Issues
Aug 11, 2009	Vulnerability in Telnet Could Allow Remote Code Execution (960859) : MS09-042	Important	No Issues
Aug 11, 2009	Vulnerability in Workstation Service Could Allow Elevation of Privilege (971657) : MS09-041	Important	No Issues
Aug 11, 2009	Vulnerability in Message Queuing Could Allow Elevation of Privilege (971032) : MS09-040	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Aug 11, 2009	Vulnerabilities in WINS Could Allow Remote Code Execution (969883) : MS09-039	Critical	No Issues
Aug 11, 2009	Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (971557) : MS09-038	Critical	No Issues
Aug 11, 2009	Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908) : MS09-037	Critical	No Issues
Jul 17, 2009	List of Changes and fixed issues in the .NET Framework 3.5 Service Pack 1 (951847) : MS08-040	Important	No Issues
Jul 14, 2009	Cumulative Security Update of ActiveX Kill Bits (973346) : MS09-032	Critical	No Issues
Jul 14, 2009	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (961371) : MS09-029	Critical	No Issues
Jul 14, 2009	Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (971633) : MS09-028	Critical	No Issues
Jun 9, 2009	Vulnerability in RPC Could Allow Elevation of Privilege (970238) : MS09-026	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Jun 9, 2009	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537) : MS09-025	Important	No Issues
Jun 9, 2009	Vulnerability in Windows Search Could Allow Information Disclosure (963093) : MS09-023	Moderate	No Issues
Jun 9, 2009	Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501) : MS09-022	Critical	No Issues
Jun 9, 2009	Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483) : MS09-020	Important	No Issues
Jun 9, 2009	Cumulative Security Update for Internet Explorer (969897) : MS09-019	Critical	No Issues
Jun 9, 2009	Vulnerabilities in Active Directory Could Allow Remote Code Execution (971055) : MS09-018	Critical	No Issues
Apr 14, 2009	Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426) : MS09-015	Moderate	No Issues
April 16, 2009	Vulnerabilities in Windows Could Allow Elevation of Privilege (959454) MS09-012	Important	Issue found – Please reference click here for details (Or view Reported Issue Section)
Apr 14, 2009	Cumulative Security Update for Internet Explorer (963027) : MS09-014	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Apr 14, 2009	Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803) : MS09-013	Critical	No Issues
Apr 14, 2009	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (961373) : MS09-011	Critical	No Issues
Mar 11, 2009	Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690) MS09-006	Important	No Issues
Feb 10, 2009	Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420) : MS09-004	Important	No Issues
Feb 10, 2009	Cumulative Security Update for Internet Explorer (961260) : MS09-002	Critical	No Issues
Jan 13, 2009	Vulnerabilities in SMB Could Allow Remote Code Execution (958687) : MS09-001	Critical	No Issues
Dec 15, 2008	SQL Server 2005 Service Pack 3 http://technet.microsoft.com/en-us/sqlserver/bb895957.aspx	N/A	No Issues
Dec 17, 2008	Security Update for Internet Explorer (960714) : MS08-078	Critical	No Issues
Dec 9, 2008	Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807) : MS08-076	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Dec 9, 2008	Cumulative Security Update for Internet Explorer (958215) : MS08-073	Critical	No Issues
Dec 9, 2008	Vulnerabilities in GDI Could Allow Remote Code Execution(956802) : MS08-071	Critical	No Issues
Nov 11, 2008	Vulnerability in SMB Could Allow Remote Code Execution (957097) : MS08-068	Critical	No Issues
Oct 23, 2008	Vulnerability in Server Service Could Allow Remote Code Execution (958644) : MS08-067	Critical	No Issues
Oct 14, 2008	Vulnerability in Server Service Could Allow Remote Code Execution (958644) MS08-067	Critical	No Issues
Oct 14, 2008	Cumulative Security Update for Internet Explorer (956390) MS08-058	Critical	No Issues
Oct 14, 2008	Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege (956803) MS08-066	Important	No Issues
Oct 14, 2008	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (954211) MS08-061	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Oct 14, 2008	Vulnerability in SMB Could Allow Remote Code Execution (957095) MS08-063	Important	No Issues
Oct 14, 2008	Vulnerability in Virtual Address Descriptor Manipulation Could Allow Elevation of Privilege (956841) MS08-064	Important	No Issues
Aug 12, 2008	Vulnerability in Event System Could Allow Remote Code Execution (950974) : MS08-049	Important	No Issues
Aug 12, 2008	Vulnerability in IPsec Policy Processing Could Allow Information Disclosure (953733) : MS08-047	Important	No Issues
Aug 12, 2008	Cumulative Security Update for Internet Explorer (953838) : MS08-045	Critical	No Issues
Jul 8, 2008	Vulnerabilities in Microsoft SQL Server Could Allow Elevation of Privilege (941203) : MS08-040	Important	No Issues
Jul 8, 2008	Vulnerabilities in DNS Could Allow Spoofing (953230) : MS08-037	Important	No Issues
Jun 10, 2008	Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service (950762) : MS08-036	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Jun 10, 2008	Vulnerability in Active Directory Could Allow Denial of Service (953235): MS08-035	Important	No Issues
Jun 10, 2008	Vulnerability in WINS Could Allow Elevation of Privilege (948745): MS08-034	Important	No Issues
Jun 10, 2008	Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service (950762): MS08-036	Important	No Issues
Jun 10, 2008	Cumulative Security Update for Internet Explorer (950759): MS08-031	Critical	No Issues
Jun 10, 2008	Vulnerabilities in DirectX Could Allow Remote Code Execution (951698): MS08-033	Critical	No Issues
Jun 10, 2008	Cumulative Security Update of ActiveX Kill Bits (950760): MS08-032	Moderate	No Issues
Thursday, April 10, 2008	Security Update for ActiveX Killbits for Windows Server 2003 (KB948881)	Important	No Issues
Thursday, April 10, 2008	Cumulative Security Update for Internet Explorer 6 for Windows Server 2003 (KB947864)	Important	No Issues
Thursday, April 10, 2008	Security Update for Windows Server 2003 (KB945553)	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Thursday, April 10, 2008	Security Update for Windows Server 2003 (KB941693)	Important	No Issues
Thursday, April 10, 2008	Security Update for Windows Server 2003 (KB944338)	Critical	No Issues
Tuesday, April 08, 2008	Microsoft .NET Framework 2.0 Service Pack 1 (KB110806)	N/A	No Issues
Mar 17, 2008	Update for Windows Server 2003 (KB948496)	Critical	No Issues
Mar 17, 2008	Windows Malicious Software Removal Tool - March 2008 (KB890830)	Important	No Issues
Feb 12, 2008	Cumulative Security Update for Internet Explorer (944533): MS08-010	Critical	No Issues
Feb 12, 2008	Vulnerability in OLE Automation Could Allow Remote Code Execution (947890): MS08-008	Critical	No Issues
Feb 12, 2008	Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code Execution (946026): MS08-007	Critical	No Issues
Feb 12, 2008	Vulnerability in Internet Information Services Could Allow Remote Code Execution (942830): MS08-006	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Feb 12, 2008	Vulnerability in Internet Information Services Could Allow Elevation of Privilege (942831) : MS08-005	Important	No Issues
Feb 12, 2008	Vulnerability in Active Directory Could Allow Denial of Service (946538) : MS08-003	Important	No Issues
Jan 8, 2008	Vulnerability in LSASS Could Allow Local Elevation of Privilege (943485) : MS08-002	Important	No Issues
Jan 8, 2008	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (941644) : MS08-001	Critical	No Issues
Dec 11, 2007	Cumulative Security Update for Internet Explorer (942615) : MS07-069	Critical	No Issues
Dec 11, 2007	Vulnerability in Windows Media File Format Could Allow Remote Code Execution (941569 and 944275) : MS07-068	Critical	No Issues
Dec 11, 2007	Vulnerabilities in DirectX Could Allow Remote Code Execution (941568) : MS07-064	Critical	No Issues
Dec 11, 2007	Vulnerability in Macrovision Driver Could Allow Local Elevation of Privilege (944653) : MS07-067	Important	No Issues
Nov 13, 2007	Vulnerability in DNS Could Allow Spoofing (941672) MS07-062	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Nov 13, 2007	Vulnerability in Windows URI Handling Could Allow Remote Code Execution (943460) MS07-061	Critical	No Issues
Oct 9,2007	Cumulative Security Update for Internet Explorer (939653) MS07-057	Critical	No Issues
Sept 11, 2007	Vulnerability in Microsoft Agent Could Allow Remote Code Execution (938827) : MS07-051	Critical	No Issues
Aug 14,2007	Vulnerability in Windows Media Player Could Allow Remote Code Execution (936782) : MS07-047	Important	No Issues
Aug 14,2007	Vulnerability in GDI Could Allow Remote Code Execution (938829) : MS07-046	Critical	No Issues
Aug 14,2007	Cumulative Security Update for Internet Explorer (937143) : MS07-045	Critical	No Issues
Aug 14,2007	Vulnerability in OLE Automation Could Allow Remote Code Execution (921503) : MS07-043	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Aug 14,2007	Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (936227) : MS07-042	Critical	No Issues
Jul 10, 2007	Vulnerability in Microsoft Internet Information Services Could Allow Remote Code Execution (939373) : MS07-041	Important	No Issues
Jul 10, 2007	Vulnerabilities in .NET Framework Could Allow Remote Code Execution (931212) : MS07-040	Critical	No Issues
Jul 10, 2007	Vulnerability in Windows Active Directory Could Allow Remote Code Execution (926122) : MS07-039	Critical	No Issues
June 2007	Vulnerability in Win32 API Could Allow Remote Code Execution (935839) MS07-035	Critical	No Issues
June 2007	Cumulative Security Update for Outlook Express and Windows Mail (929123) MS07-034	Critical	No Issues
June 2007	Cumulative Security Update for Internet Explorer (933566) MS07-033	Critical	No Issues
June 2007	Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution (935840) MS07-031	Critical	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
May 8, 2007	Vulnerability in RPC on Windows DNS Server Could Allow Remote Code Execution (935966) MS07-029	Critical	No Issues
May 8, 2007	Cumulative Security Update for Internet Explorer (931768) MS07-027	Critical	No Issues
Apr. 10, 2007	Microsoft Windows Server 2003 SP 2	Important	No Issues
Apr. 10, 2007	Vulnerability in Windows Kernel Could Allow Elevation of Privilege (931784) MS07-022	Important	No Issues
Apr. 10, 2007	Vulnerabilities in CSRSS Could Allow Remote Code Execution (930178) MS07-021	Critical	No Issues
Apr. 10, 2007	Vulnerability in Microsoft Agent Could Allow Remote Code Execution (932168) MS07-020	Critical	No Issues
Apr. 10, 2007	Vulnerability in Universal Plug and Play Could Allow Remote Code Execution (931261) MS07-019	Critical	No Issues
Apr. 10, 2007	Vulnerabilities in Microsoft Content Management Server Could Allow Remote Code Execution (925939) MS07-018	N/A	N/A

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Apr. 10, 2007	Vulnerabilities in GDI Could Allow Remote Code Execution (925902) MS07-017	Critical	No Issues
Apr. 10, 2007	SQL SERVER 2005 SP2	Critical	No Issues
Feb. 13, 2007	Cumulative Security Update for Internet Explorer (928090): MS07-016	Critical	No Issues
Feb. 13, 2007	Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution (918118): MS07-013	Important	No Issues
Feb. 13, 2007	Vulnerability in Microsoft MFC Could Allow Remote Code Execution (924667): MS07-012	Important	No Issues
Feb. 13, 2007	Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (926436): MS07-011	Important	No Issues
Feb. 13, 2007	Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (927779): MS07-009	Critical	No Issues
Feb. 13, 2007	Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843): MS07-008	Critical	No Issues
Feb. 13, 2007	Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege (927802): MS07-007	Important	No Issues

MICROS Confidential

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.

Date	Bulletin Description	Severity	Results
Feb. 13, 2007	Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255) : MS07-006	Important	No Issues
Feb. 13, 2007	Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (923723) : MS07-005	Important	No Issues
Jan. 9, 2007	Vulnerability in Vector Markup Language Could Allow Remote Code Execution (929969) : MS07-004	Critical	No Issues

MICROS Confidential

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.

Reported Issues

MS patch KB956572 causing OperaLogin to crash (sometimes)

The following is still a work in progress. If anybody sees any sign of this issue, please contact me with the details as we currently still have an open support ticket with Oracle on this item.

The workaround described at the end of this email should be considered just a temporary workaround and not a permanent fix. Please do not make these changes on servers that are not experiencing the problem described.

Micros Fidelio France office reported that after applying Microsoft Security bundle MS09-012, which was rolled out in auto-updates last week, the app server would no longer work. They were getting HTTP-500 errors when connecting to OperaLogin.

The issue could be seen as an error in the OperaLogin application log that said the following;

```
<H3>Erreurs de compilation :D:\oracle\10gappr2\j2ee\OC4J_BI_Forms\application-deployments\OperaLogin\OperaLogin\persistence\_pages\_web_2d_inf\_jsp\_welcome.java</H3>  
<pre>Error occurred during initialization of VM  
Could not reserve enough space for object heap  
</pre>
```

They also reported that uninstalling KB956572 from that patch bundle would resolve the problem.

A couple years ago, we saw the same problems after the rollout of MS06-040 bundle with patch KB921883. Microsoft quickly released a hotfix to resolve the issue.

This older issue is documented here;

Oracle Metalink Doc ID: 388379.1

Microsoft KB article: <http://support.microsoft.com/kb/924054>

Sun Java Forums: <http://forum.java.sun.com/thread.jspa?threadID=759413>

Some testing on these Fidelio France servers resulted in finding a bit of information that was also reported in some Internet forums found via Google searches. Setting the OC4J's max memory heap values (-Xmx setting) to 1024m or higher would prevent the OC4J from starting.

Going back to the original error, it points at a problem compiling the JSP pages. Based on info from Metalink articles, we configured a limit the memory allocated to the JAVAC (java compiler) command line that the OC4J uses to compile JSP pages.

In the \oracle\10gappr2\j2ee\oc4j_bi_forms\config\server.xml, the following line;

MICROS Confidential

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.

```
<java-compiler name="javac" in-process="false" extdirs="D:\oracle\10gappr2\jdk\jre\lib\ext" />
```

Was changed to;

```
<java-compiler name="javac" in-process="false" options="-J -Xmx750m -encoding UTF8" extdirs="D:\oracle\10gappr2\jdk\jre\lib\ext" />
```

After restarting the services, everything appears to be working.

We currently have Oracle SR #7546362.992 open on this issue.

So far, we have only seen this on installs of “Microsoft Windows 2003 Server – French edition”

MICROS Confidential

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.

General Information

Unexplained Database Slowdown Seen on Windows 2003 Service Pack 1

Applies to:

Oracle Server - Enterprise Edition - Version: 9.2 to 11.1
Microsoft Windows Server 2003 (64-bit Itanium)
Microsoft Windows Server 2003
Microsoft Windows XP (64-bit AMD64 and Intel EM64T)

Description

Periodic Database slowdowns seen in Windows 2003 environments with lots of memory, running Service Pack 1

Likelihood of Occurrence

Environments with a high level of concurrency, many CPU's and large amounts of physical ram are prone to this type of problem.

Possible Symptoms

Symptoms

Symptoms include any or all of the following:

1. General slowdowns in the database, which may appear to be hung, even though systemstate dumps may not show evidence of hangs or locking contention. Sometimes, the database may recover from these slowdowns on its own, and begin responding with no user intervention. At other times, the database may appear to be hung for long periods of time.
2. Other symptoms may include slow disk I/O - i.e. a large increase in average I/O times may be observed when reviewing AWR reports covering the time period in question.
3. It may also be observed that network latency increases dramatically. If running in a RAC environment, you may notice an increase in cluster latency - i.e. an increase in the wait times for global cache requests and messages (again, as observed in AWR reports or in some cases as seen via real-time monitoring tools).
4. If running in a RAC environment, we may see IPC timeouts in the ipcdbg logfiles.

See MetaLink Note 464683.1 for details.

MICROS Confidential

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.

Missing "Help and Support" service after Windows 2003 SP2

This has come up a couple times over the last couple days. It appears that after the Windows 2003 Server SP2 gets applied, the "Help and Support" service is sometimes missing. Among other things, with this service not running prevents "System Information" utility from running. We're not sure how many other things are affected. The resolution for the moment is documented in these steps.

Help and Support Error

Windows cannot open Help and Support because a system service is not running.

To fix this problem, start the service named 'Help and Support'.

OK

This issue is currently under investigation, however if you are currently experiencing this issue you can run the following commands to resolve the issue:

1. Open a command prompt.
2. Navigate to %windir%\PCHealth\HelpCtr\Binaries
3. Run "start /w helpsvc /svchost netsvcs /regserver /install"
4. Once this command completes the Help and Support service should now appear in services.msc
5. Start the Help and Support service

MICROS Confidential

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.

Potential problem with Windows XP SP3 on non-Intel machines

There have been some reports of problems with Windows XP SP3 on non Intel machines. The issues appear to affect a great deal of HP workstations running AMD processors. Several websites have details on the issues and further details.

It appears the problem has to do with how some manufacturer's image the operating system with sysprep. Microsoft has provided the following knowledge base article on how to resolve some of the issues.

<http://support.microsoft.com/kb/888372>

If anybody has encountered issues with this SP, we'd appreciate hearing back on some of the details and if the information in this article is accurate and resolved the problems.

Issue with large memory systems running Windows 2003 SP1

We recently encountered an issue at a site running Oracle 10gR2 on Windows 2003 SP1. The issue caused some system hangs resulting in outages for the client.

After some detailed investigations, the issue was found to be a result of the problem documented in the following Microsoft knowledge base article.

<http://support.microsoft.com/kb/919341/en-us>

This issue appears to only affect Windows systems with very large amounts of memory. It is unknown how much memory is required to encounter this bug however this particular environment had 64gig of physical RAM on the servers.

For large memory environments we recommend validating that the patch in the above article has been applied. The fix is available as a one-off and was also included in Windows 2003 SP2.

Critical update testing has not been and will not be performed with versions of RES3000 prior to v3.1. Updates to these systems should be applied with caution and at your own risk. NO WARRANTIES OF ANY KIND OR NATURE ARE PROVIDED IF YOU ELECT TO UPDATE YOUR SYSTEM. THE PRODUCTS ARE PROVIDED WHERE IS, AS IS, WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PRODUCT IS WITH YOU. MICRO DOES NOT WARRANT THAT THE PERFORMANCE OF THE PRODUCTS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PRODUCTS WILL BE UNINTERRUPTED OR ERROR FREE. IN NO EVENT SHALL MICROS BE RESPONSIBLE FOR ANY DAMAGES, INCLUDING DIRECT DAMAGES, ANY LOST SAVINGS OR PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES.

MICROS' recommendation to our users on versions prior to v.3.1 software is to develop a security strategy that works for your business model. I.e., Private Networks, Firewall. If you feel you need to apply **any** Microsoft updates to these RES3000 versions, you should do so in a controlled lab environment thoroughly testing prior to any deployment.

MICROS Confidential

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.

MICROS Confidential

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.