BeyondTrust 2010 Microsoft Vulnerability Report

Abstract

This BeyondTrust report investigates all vulnerabilities published in Microsoft's 2010 Security Bulletins, as well as all of the published Windows 7 vulnerabilities to date. It reports on vulnerabilities that are mitigated by configuring users to operate without administrator rights, and examines the latest major Microsoft releases. The results show that despite attacks that are unpredictable and evolving in nature, companies can greatly reduce risk, experience greater protection from zero-day threats, and reduce the threat from vulnerabilities by removing administrator rights.

beyondtrust
privilege. made simple

www.beyondtrust.com

BeyondTrust
2173 Salk Avenue
Carlsbad, California 92008
Phone: +1 818-575-4000

Table of Contents

Executive Summary

Microsoft and its partners regularly identify new security vulnerabilities in Microsoft software. In 2010 Microsoft published over 100 security bulletins documenting and providing patches for 256 vulnerabilities. BeyondTrust examined and analyzed all of the published Microsoft vulnerabilities in 2010 and all of the published Windows 7 vulnerabilities to date, allowing this report to accurately quantify the continued effectiveness of removing administrator rights at mitigating vulnerabilities in Microsoft software. Key findings from this report show that removing administrator rights will better protect companies against the exploitation of:

•75% of Critical Windows 7 vulnerabilities reported by Microsoft to date
• 100% of Microsoft Office vulnerabilities reported in 2010
• 100% of Internet Explorer and IE 8 vulnerabilities reported in 2010
• 64% of all Microsoft vulnerabilities reported in 2010

Microsoft is to be lauded for releasing patches to known vulnerabilities each month. Vulnerabilities, however, take time to identify. Patches can take even longer to apply. During this down period, threats can damage a corporate network and gain access to sensitive information. A Privilege Identity Management solution that eliminates administrator rights from desktop users will substantially reduce the severity and/or prevent the exploitation of undiscovered or unpatched vulnerabilities. Enterprises should ensure that while administrative rights are removed to protect desktops from these vulnerabilities, users can also continue to operate effectively and with access to required applications.

About the Data Collection and Analysis

Microsoft publishes a Security Bulletin Summary each month to notify customers of security updates made to address vulnerabilities in its products. The security updates are released on the second Tuesday of the month, a day commonly known as Patch Tuesday. Individual Security Bulletins, identified within the monthly summaries, each describe a set of vulnerabilities and are linked to from the Security Bulletin Summary page. The following Web page contains links to all of the Microsoft Security Bulletin Summaries for 2010:

http://www.microsoft.com/technet/security/bulletin/summary.mspx#ERC.

Table 1, located in the Appendix, contains a list of all Security Bulletins and vulnerabilities published in 2010.

Table 2 contains a list of all Windows 7 vulnerabilities published in Security Bulletins to date.

This report uses information found in the Individual Security Bulletins to classify vulnerabilities by Severity Rating, Vulnerability Impact, and Affected Software. It also determines if removing administrator rights could mitigate a vulnerability to the Microsoft product (s). A vulnerability is considered mitigated by removing administrator rights if the following sentence is located in the Security Bulletin's Mitigating Factors section, "Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights."

Section 1: Analysis of All 2010 Microsoft Vulnerabilities

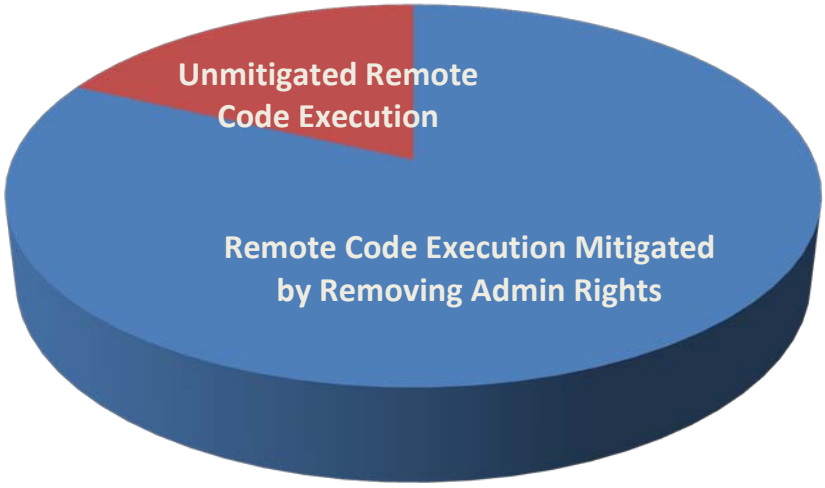
100% of Microsoft Office Vulnerabilities are Mitigated by Configuring Users to Operate Without Administrator Rights.

Microsoft Office provides some of the most widely used software applications in the world. Given the prevalence of the software and the number of vulnerabilities, increased security protection is key. A total of 84 Microsoft Office vulnerabilities appeared in the 2010 Security Bulletins. Of these, all 84 are mitigated by removing administrator rights.

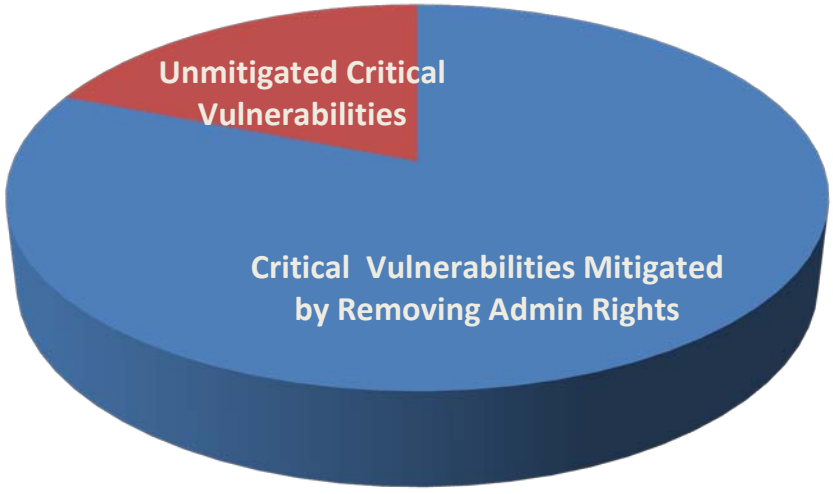
By Removing Administrator Rights, Companies will be Better Protected Against Exploitation of 100% of Vulnerabilities in all Versions of Internet Explorer, including those in IE 8.

Microsoft released Internet Explorer 9 in March of 2011. It is regarded as the most secure version of the browser, and no vulnerabilities have yet to be reported. Prior to Internet Explorer 9 was Internet Explorer 8. In 2010, there were 43 reported Internet Explorer vulnerabilities. 100% of the Internet Explorer , including IE 8, vulnerabilities can be mitigated by removing administrator rights.

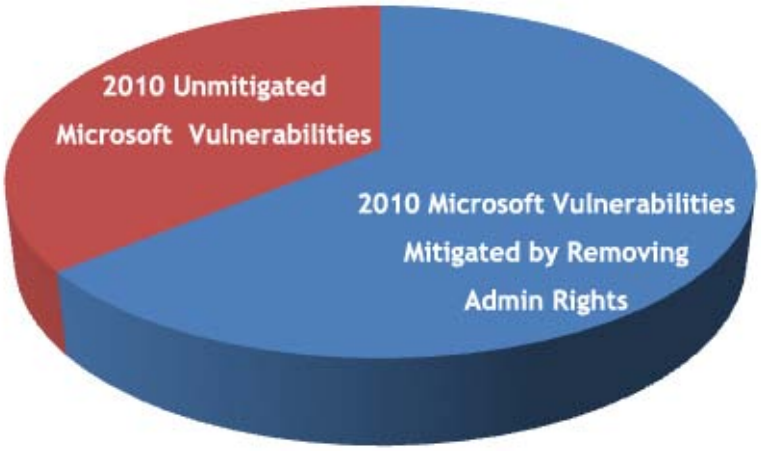
82% of Vulnerabilities Categorized as Remote Code Execution are Mitigated by Removing Administrator Rights. A vulnerability impact rating is assigned to each Microsoft Security Bulletin and indicates the effect an exploit of the vulnerabilities may have. Remote Code Execution vulnerabilities may allow someone who is not at the computer to run unauthorized software and install programs; view, change, or delete data; and/or create new user accounts. In 2010, there were 192 Remote Code Execution Microsoft vulnerabilities published, with 158 of them mitigated by removing administrator rights.



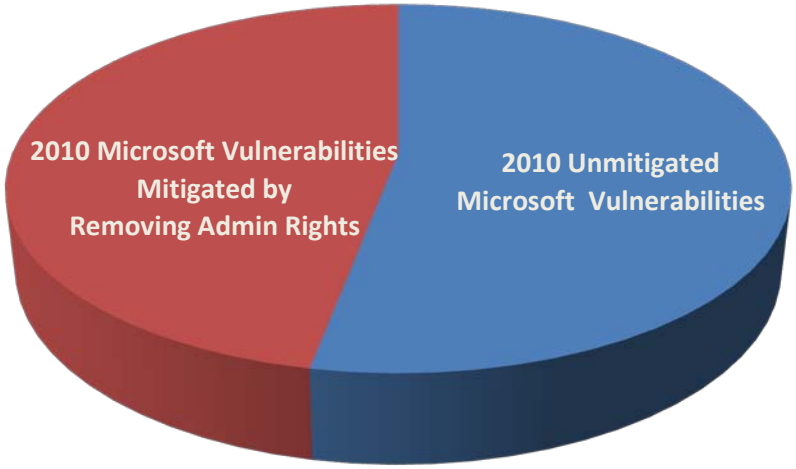
Companies are Better Protected Against 81% of Critical Microsoft Vulnerabilities by Configuring Users Without Administrator Rights. Each Microsoft Security Bulletin is given a severity rating. Critical is the highest rating and indicates that the vulnerabilities are of the highest security concern. In total 101 vulnerabilities appeared in 2010 Security Bulletins with a critical rating and 82 of these are mitigated by removing administrator rights.



Of the Total Published Microsoft Vulnerabilities, 64% are Mitigated by Removing Administrator Rights. In 2010 there were 256 vulnerabilities published by Microsoft in Security Bulletins. Companies would be better protected against exploitation of 163 of these vulnerabilities by eliminating administrator rights.

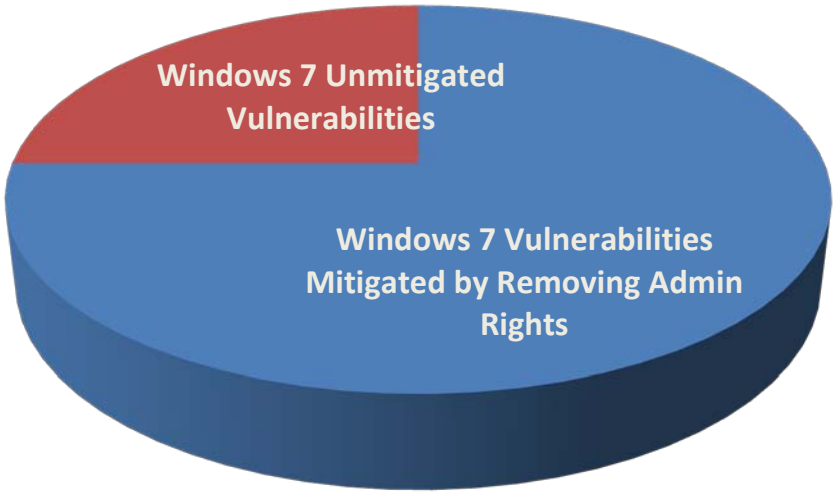


In 2010, Exploits of 47% of Windows Operating System Vulnerabilities Could Be Diminished by Configuring Users as Standard Users. In 2010 there were 162 published vulnerabilities for all versions of Microsoft operating systems. Companies would be better protected against exploitation of 76 of these vulnerabilities by removing administrator rights.

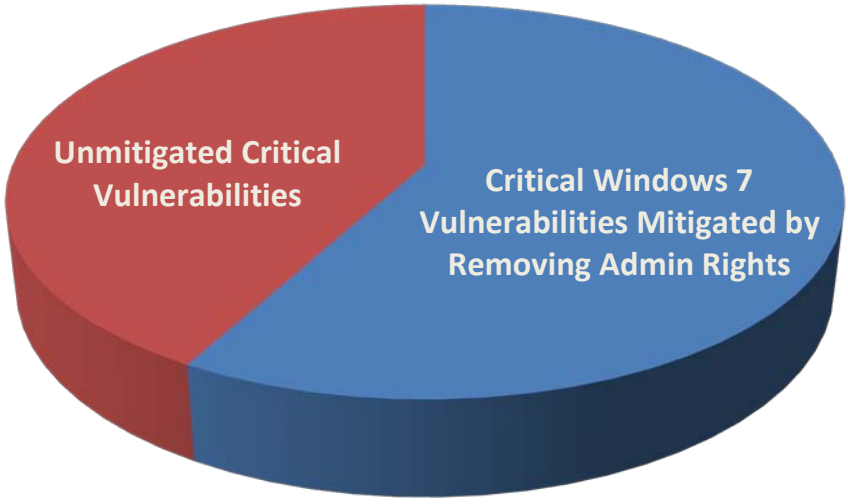


Section 2: Analysis of All Windows 7 Vulnerabilities to Date

75% of Critical Windows 7 Operating System Vulnerabilities are Mitigated by Having Users Log in as Standard Users. Since the October 2009 release of Windows 7 there have been 72 Critical Windows 7 operating system vulnerabilities published. Companies would be better protected against exploitation of 54 of the Critical Windows 7 vulnerabilities by eliminating administrator rights.



Of all Windows 7 Vulnerabilities Ever Published, 42% are Mitigated by Removing Administrator Rights. There have been a total of 147 Windows 7 vulnerabilities published to date. The first vulnerability was published in October 2009, when Windows 7 was publically released. This report captures all Windows 7 vulnerabilities published through March 2011. To date, 62 vulnerabilities are mitigated by removing administrator rights.



Conclusion

Microsoft does a commendable job of publically disclosing detailed information about vulnerabilities and providing patches every month. However, software vulnerabilities take time to identify, and patches take time to apply. It is during this period of time that exploits of unpatched or undiscovered vulnerabilities can damage a corporate network and gain access to sensitive information. This report demonstrates the critical role that restricting administrator rights plays in protecting against vulnerabilities. It is important to note that this increased protection is achievable in one simple step without any impact on productivity — by implementing a desktop Privilege Identity Management solution. As companies roll out Windows 7 they need to include plans to implement a desktop Privilege Identity Management solution in order to reduce the severity or prevent the exploitation of undiscovered or unpatched vulnerabilities and to ensure that their users can operate effectively without administrator rights.

About BeyondTrust

BeyondTrust empowers IT to eliminate the risk of intentional, accidental and indirect misuse of privileges on desktops and servers with globally proven solutions that increase security and compliance without impacting productivity. With over 25 years of global success, BeyondTrust is the pioneer of solutions for privileged identity management in heterogeneous IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises. Customers include eight of the world's 10 largest banks, seven of the world's 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities. The company is privately held and headquartered in Carlsbad, California, with an office in Los Angeles, California, the Greater Boston area, as well as EMEA offices in London, UK. For more information, visit www.beyondtrust.com.

About PowerBroker for Desktops

BeyondTrust PowerBroker for Desktops, initially released in 2004, is the first Least Privilege Management solution for Windows. PowerBroker for Desktops allows end-users to run all required applications, processes and ActiveX controls without administrative privileges. PowerBroker for Desktops allows network administrators to attach permission levels to Windows applications to enforce enterprise security policy while still enabling users to perform approved activities. By removing the need to grant administrative rights to end-users, IT departments eliminate what is otherwise the Achilles heel of the desktop – end-users with administrative power that can be exploited by malware and malicious intent to change security settings and disable other security solutions. PowerBroker for Desktops is easy to implement. It plugs directly into Group Policy, the existing Windows security infrastructure. It is transparent to the end-user, without pop-ups or dialogue boxes, and supports Windows 2000, XP, Server 2003, Server 2008, Vista and Windows 7.

Appendix A- 2010 Microsoft Vulnerabilities

Date	Bulletin ID	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Jan-10	**MS10-001**	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)	Microtype Express Compressed Fonts Integer Flaw in the LZCOMP Decompressor Vulnerability- CVE-2010-0018	Critical	Remote Code Execution	Windows 2000, Windows Server, Windows XP, Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	Yes
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	XSS Filter Script Handling Vulnerability (CVE-2009-4074)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000 Professional, Windows 2000 Server, Internet Explorer 6, Internet Explorer 7, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0	Yes
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	URL Validation Vulnerability (CVE-2010-0027)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000 Professional, Windows 2000 Server, Internet Explorer 6, Internet Explorer 7, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0	Yes
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	HTML Object Memory Corruption Vulnerability (CVE-2010-0249)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000 Professional, Windows 2000 Server, Internet Explorer 6, Internet Explorer 7, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0	Yes
Jan-	**MS10-002**	Cumulative Security	HTML Object	Critical	Remote Code	Internet Explorer 5.01,	Yes

10		Update for Internet Explorer (978207)	Memory Corruption Vulnerability (CVE-2010-0248)		Execution	Windows 2000 Server, Windows 2000 Professional, Windows 2000 Server, Internet Explorer 6, Internet Explorer 7, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0	
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	Uninitialized Memory Corruption Vulnerability (CVE-2010-0247)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000 Professional, Windows 2000 Server, Internet Explorer 6, Internet Explorer 7, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0	Yes
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	Uninitialized Memory Corruption Vulnerability (CVE-2010-0246)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000 Professional, Windows 2000 Server, Internet Explorer 6, Internet Explorer 7, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0	Yes
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	Uninitialized Memory Corruption Vulnerability (CVE-2010-0245)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000 Professional, Windows 2000 Server, Internet Explorer 6, Internet Explorer 7, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0	Yes
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	Uninitialized Memory Corruption Vulnerability (CVE-2010-0244)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000 Professional, Windows 2000 Server, Internet Explorer 6, Internet Explorer 7, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0	Yes
Feb-10	**MS10-003**	Vulnerability in Microsoft Office (MSO) Could Allow Remote Code Execution (978214)	MSO.DLL Buffer Overflow Vulnerability (CVE-2010-0243)	Important	Remote Code Execution	Office 2004 for Macintosh Gold, Office XP SP3	Yes
Feb-10	**MS10-004**	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (975416)	PowerPoint File Path Handling Buffer Overflow (CVE-2010-0029)	Important	Remote Code Execution	Office 2004 for Macintosh, PowerPoint 2003, Office 2003, PowerPoint 2002, Office XP	Yes
Feb-10	**MS10-004**	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code	PowerPoint LinkedSlideAtom Heap Overflow Vulnerability (CVE-2010-0030)	Important	Remote Code Execution	Office 2004 for Macintosh, PowerPoint 2003, Office 2003, PowerPoint 2002, Office XP	Yes

		Execution (975416)					
Feb-10	**MS10-004**	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (975416)	PowerPoint OEPlaceholderAtom 'placementId' Invalid Array Indexing Vulnerability (CVE-2010-0031)	Important	Remote Code Execution	Office 2004 for Macintosh, PowerPoint 2003, Office 2003, PowerPoint 2002, Office XP	Yes
Feb-10	**MS10-004**	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (975416)	PowerPoint OEPlaceholderAtom Use After Free Vulnerability (CVE-2010-0032)	Important	Remote Code Execution	Office 2004 for Macintosh, PowerPoint 2003, Office 2003, PowerPoint 2002, Office XP	Yes
Feb-10	**MS10-004**	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (975416)	PowerPoint Viewer TextBytesAtom Record Stack Overflow Vulnerability (CVE-2010-0033)	Important	Remote Code Execution	Office 2004 for Macintosh, PowerPoint 2003, Office 2003, PowerPoint 2002, Office XP	Yes
Feb-10	**MS10-004**	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (975416)	Office PowerPoint Viewer TextCharsAtom Record Stack Overflow (CVE-2010-0034)	Important	Remote Code Execution	Office 2004 for Macintosh, PowerPoint 2003, Office 2003, PowerPoint 2002, Office XP	Yes
Feb-10	**MS10-005**	Vulnerability in Microsoft Paint Could Allow Remote Code Execution (978706)	MSPaint Integer Overflow Vulnerability (CVE-2010-0028)	Moderate	Remote Code Execution	Windows 2000 l, Windows 2000 Server, Windows Server 2003, Windows XP	Yes
Feb-10	**MS10-006**	Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)	SMB Client Pool Corruption Vulnerability (CVE-2010-0016)	Critical	Remote Code Execution	Windows 2000, Windows 2000 Server, Windows Server 2008, Windows XP, Windows Vista, Windows Server 2003, Windows 7	No
Feb-10	**MS10-006**	Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)	SMB Client Race Condition Vulnerability (CVE-2010-0017)	Critical	Remote Code Execution	Windows 2000, Windows 2000 Server, Windows Server 2008, Windows XP, Windows Vista, Windows Server 2003, Windows 7	No
Feb-10	**MS10-007**	Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (975713)	URL Validation Vulnerability (CVE-2010-0027)	Critical	Remote Code Execution	Windows 2000, Windows 2000 Server, Windows XP, Windows Server 2003	Yes
Feb-10	**MS10-008**	Cumulative Security Update of ActiveX Kill Bits (978262)	Microsoft Data Analyzer ActiveX Control Vulnerability (CVE-2010-0252)	Critical	Active X Kill Bits	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003, Windows 7, Windows Server 2008, Windows Vista,	Yes
Feb-10	**MS10-009**	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	ICMPv6 Router Advertisement Vulnerability (CVE-2010-0239)	Critical	Remote Code Execution	Windows Vista, Windows Server 2008	No

Feb-10	**MS10-009**	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	Header MDL Fragmentation Vulnerability (CVE-2010-0240)	Critical	Remote Code Execution	Windows Vista, Windows Server 2008	No
Feb-10	**MS10-009**	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (974145)	ICMPv6 Route Information Vulnerability (CVE-2010-0241)	Critical	Remote Code Execution	Windows Vista, Windows Server 2008	No
Feb-10	**MS10-010**	Vulnerability in Windows Server 2008 Hyper-V Could Allow Denial of Service (977894)	Hyper-V Instruction Set Validation Vulnerability (CVE-2010-0026)	Important	Denial of Service	Windows Server 2008	No
Feb-10	**MS10-011**	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (978037)	CSRSS Local Privilege Elevation Vulnerability (CVE-2010-0023)	Important	Elevation of Privilege	Windows 2000, Windows 2000 Server, Windows XP, Windows Server 2003	No
Feb-10	**MS10-012**	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	SMB Pathname Overflow Vulnerability (CVE-2010-0020)	Important	Remote Code Execution	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows XP, Windows 7, Windows Server 2008, Windows Vista,	No
Feb-10	**MS10-012**	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	SMB Memory Corruption Vulnerability (CVE-2010-0021)	Important	Remote Code Execution	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows XP, Windows 7, Windows Server 2008, Windows Vista,	No
Feb-10	**MS10-012**	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	SMB NTLM Authentication Lack of Entropy Vulnerability (CVE-2010-0231)	Important	Remote Code Execution	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows XP, Windows 7, Windows Server 2008, Windows Vista,	No
Feb-10	**MS10-013**	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935)	DirectShow Heap Overflow Vulnerability (CVE-2010-0250)	Critical	Remote Code Execution	Windows 2000, Server Windows 2000 Windows XP, Windows Server 2003, Windows 7, Windows Server 2008, Windows Vista,	Yes
Feb-10	**MS10-014**	Vulnerability in Kerberos Could Allow Denial of Service (977290)	Kerberos Null Pointer Dereference Vulnerability – CVE- 2010-0035	Important	Denial of Service	Windows 2000 , Windows 2000 Server, Windows Server 2003, Windows Server 2008,	No
Feb-10	**MS10-015**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)	Windows Kernel Double Free Vulnerability (CVE-2010-0233)	Important	Elevation of Privilege	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Mar-10	**MS10-016**	Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (975561)	Movie Maker and Producer Buffer Overflow Vulnerability (CVE-2010-	Important	Remote Code Execution	Windows XP, Windows Vista, Windows 7 Microsoft Producer 2003	Yes

			0265)				
Mar-10	**MS10-017**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)	Microsoft Office Excel Record Memory Corruption Vulnerability (CVE-2010-0257)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Office SharePoint Server 2007	Yes
Mar-10	**MS10-017**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)	Microsoft Office Excel Sheet Object Type Confusion Vulnerability (CVE-2010-0258)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Office SharePoint Server 2007	Yes
Mar-10	**MS10-017**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)	Microsoft Office Excel MDXTUPLE Record Heap Overflow Vulnerability (CVE-2010-0260)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Office SharePoint Server 2007	Yes
Mar-10	**MS10-017**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)	Microsoft Office Excel MDXSET Record Heap Overflow Vulnerability (CVE-2010-0261)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Office SharePoint Server 2007	Yes
Mar-10	**MS10-017**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)	Microsoft Office Excel FNGROUPNAME Record Uninitialized Memory Vulnerability (CVE-2010-0262)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Office SharePoint Server 2007	Yes

Mar-10	**MS10-017**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)	Microsoft Office Excel XLSX File Parsing Code Execution Vulnerability (CVE-2010-0263)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Office SharePoint Server 2007	Yes
Mar-10	**MS10-017**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)	Microsoft Office Excel DbOrParamQry Record Parsing Vulnerability (CVE-2010-0264)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Office SharePoint Server 2007	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	Uninitialized Memory Corruption Vulnerability (CVE-2010-0267)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	Post Encoding Information Disclosure Vulnerability (CVE-2010-0488)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	Uninitialized Memory Corruption Vulnerability (CVE-2010-0490)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	HTML Object Memory Corruption Vulnerability (CVE-2010-0491)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-	**MS10-018**	Cumulative Security	HTML Object Memory	Critical	Remote Code	Internet Explorer 5.01, Windows 2000 Server,	Yes

10		Update for Internet Explorer (980182)	Corruption Vulnerability (CVE-2010-0492)		Execution	Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	HTML Element Cross-Domain Vulnerability (CVE-2010-0494)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	Memory Corruption Vulnerability (CVE-2010-0805)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	Uninitialized Memory Corruption Vulnerability (CVE-2010-0806)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	HTML Rendering Memory Corruption Vulnerability (CVE-2010-0807)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Apr-10	**MS10-019**	Vulnerabilities in Windows Could Allow Remote Code Execution (981210)	WinVerify Trust Signature Validation Vulnerability-CVE-2010-0486	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Apr-10	**MS10-019**	Vulnerabilities in Windows Could Allow Remote Code Execution (981210)	Cabview Corruption Validation Vulnerability-CVE-2010-0487	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Apr-10	**MS10-020**	Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)	SMB Client Memory Allocation Vulnerability (CVE-2010-0269)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7 Windows Server 2008	No
Apr-10	**MS10-020**	Vulnerabilities in SMB Client Could Allow	SMB Client Transaction	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows	No

		Remote Code Execution (980232)	Vulnerability (CVE-2010-0270)			XP, Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7 Windows Server 2008	
Apr-10	**MS10-020**	Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)	SMB Client Response Parsing Vulnerability (CVE-2010-0476)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7 Windows Server 2008	No
Apr-10	**MS10-020**	Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)	SMB Client Message Size Vulnerability (CVE-2010-0477)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Null Pointer Vulnerability(CVE-2010-0234)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Symbolic Link Value Vulnerability (CVE-2010-0235)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Memory Allocation Vulnerability (CVE-2010-0236)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Symbolic Link Creation Vulnerability (CVE-2010-0237)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Registry Key Vulnerability (CVE-2010-0238)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Virtual Path Parsing Vulnerability (CVE-2010-0481)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Malformed Image Vulnerability (CVE-2010-0482)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Exception Handler Vulnerability (CVE-2010-0810)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No

Apr-10	**MS10-022**	Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (981169)	VBScript Help Keypress Vulnerability – CVE-2010-0483	Important	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	Yes
Apr-10	**MS10-023**	Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (981160)	Microsoft Office Publisher File Conversion TextBox Processing Buffer Overflow Vulnerability (CVE-2010-0479)	Important	Remote Code Execution	Office XP, Publisher 2002, Office 2003, Publisher 2003, Outlook 2000, Publisher 2007, Office System 2007	Yes
Apr-10	**MS10-024**	Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832)	SMTP Server MX Record Vulnerability- CVE-2010-0024	Important	Denial of Service	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003 Windows Server 2008, Exchange 2000 Server, Exchange Server 2003, Exchange Server 2007, Exchange Server 2010	No
Apr-10	**MS10-024**	Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832)	SMTP Memory Allocation Vulnerability- CVE-2010-0025	Important	Denial of Service	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003 Windows Server 2008, Exchange 2000 Server, Exchange Server 2003, Exchange Server 2007, Exchange Server 2010	No
Apr-10	**MS10-025**	Vulnerability in Microsoft Windows Media Services Could Allow Remote Code Execution (980858)	Media Services Stack-based Buffer Overflow Vulnerability (CVE-2010-0478)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000	No
Apr-10	**MS10-026**	Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (977816)	MPEG Layer-3 Audio Decoder Stack Overflow Vulnerability (CVE-2010-0480)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003 Datacenter Edition, Windows Vista, Windows Server 2008	Yes
Apr-10	**MS10-027**	Vulnerability in Windows Media Player Could Allow Remote Code Execution (979402)	Media Player Remote Code Execution Vulnerability (CVE-2010-0268)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows Media Player 9.0, Windows XP	Yes
Apr-10	**MS10-028**	Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (980094)	Visio Attribute Validation Memory Corruption Vulnerability (CVE-2010-0254)	Important	Remote Code Execution	Visio 2002, Visio 2003, Visio 2007	Yes
Apr-10	**MS10-028**	Vulnerabilities in Microsoft Visio Could Allow Remote Code	Visio Index Calculation Memory Corruption	Important	Remote Code Execution	Visio 2002, Visio 2003, Visio 2007	Yes

		Execution (980094)	Vulnerability (CVE-2010-0256)				
Apr-10	**MS10-029**	Vulnerability in Windows ISATAP Component Could Allow Spoofing (978338)	ISATAP IPv6 Source Address Spoofing Vulnerability (CVE-2010-0812)	Moderate	Spoofing	Windows XP, Windows Server 2003 Windows Vista, Windows Server 2008,	No
May-10	**MS10-030**	Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)	Windows Mail Client Integer Overflow Vulnerability (CVE-2010-0816)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Outlook Express 5.5, Outlook Express 6, Windows XP, Windows Live Mail, Windows Mail, Windows Vista, Windows Server 2003, Windows Server 2008, Windows 7	Yes
May-10	**MS10-031**	Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (978213)	VBE6.dll Stack Memory Corruption Vulnerability (CVE-2010-0815)	Critical	Remote Code Execution	Office XP, Office 2003, Office System 2007	Yes
Jun-10	**MS10-032**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)	Win32k Improper Data Validation Vulnerability (CVE-2010-0484)	Important	Elevation of Privilege	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	No
Jun-10	**MS10-032**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)	Win32k TrueType Font Parsing Vulnerability (CVE-2010-1255)	Important	Elevation of Privilege	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	No
Jun-10	**MS10-033**	Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)	Media Decompression Vulnerability (CVE-2010-1879)	Critical	Remote Code Execution	Windows Server 2003, Windows XP Windows 2000 Advanced Server, Windows 2000, Windows Media Encoder 9 Series, Windows Vista, Windows Server 2008 Windows 7	Yes
Jun-10	**MS10-033**	Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)	MJEP Media Decompression Vulnerability (CVE-2010-1880)	Critical	Remote Code Execution	Windows Server 2003, Windows XP Windows 2000 Advanced Server, Windows 2000, Windows Media Encoder 9 Series, Windows Vista, Windows Server 2008 Windows 7	Yes
Jun-10	**MS10-034**	Cumulative Security Update of ActiveX Kill Bits (980195)	Microsoft Data Analyzer ActiveX Control Vulnerability (CVE-2010-0252)	Critical	Active X Kill Bits	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	Yes
Jun-10	**MS10-034**	Cumulative Security Update of ActiveX Kill Bits (980195)	Microsoft internet Explorer 8 Developer Tools Vulnerability (CVE-2010-0811)	Critical	Active X Kill Bits	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	Yes
Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	toStaticHTML Information Disclosure Vulnerability (CVE-2010-1257)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows	Yes

						Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	
Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	toStaticHTML Information Disclosure Vulnerability (CVE-2010-1257)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	Yes
Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	Uninitialized Memory Corruption Vulnerability (CVE-2010-1259)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	Yes
Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	HTML Element Memory Corruption Vulnerability (CVE-2010-1260)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	Yes
Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	Uninitialized Memory Corruption Vulnerability (CVE-2010-1261)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	Yes
Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	Memory Corruption Vulnerability (CVE-2010-1262)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	Yes
Jun-10	**MS10-036**	Vulnerability in COM Validation in Microsoft Office Could Allow Remote Code Execution (983235)	COM Validation Vulnerability (CVE-2010-1263)	Important	Remote Code Execution	Office XP, Office 2003, Excel 2003, PowerPoint 2003, Publisher 2003, Visio 2003, Word 2003, Office System 2007, Excel 2007, PowerPoint 2007, Visio 2007, Word 2007, Publisher 2007	Yes
June-10	**MS10-037**	Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)	OpenType CFF Font Driver Memory Corruption Vulnerability (CVE-2010-0819)	Important	Elevation of Privilege	Windows 2000 Server, Windows 2000, Windows XP, Windows Vista, Windows Server 2003 Windows Server 2008, Windows 7	No
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote	Excel Record Parsing Memory Corruption Vulnerability	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office	Yes

		Code Execution (2027452)	(CVE-2010-0821)			Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel Object Stack Overflow Vulnerability (CVE-2010-0822)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel Memory Corruption Vulnerability (CVE-2010-0823)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel Record Memory Corruption Vulnerability (CVE-2010-0824)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel Record Memory Corruption Vulnerability (CVE-2010-1245)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel RTD Memory Corruption Vulnerability (CVE-2010-1246)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes

Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel Memory Corruption Vulnerability (CVE-2010-1247)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel HFPicture Memory Corruption Vulnerability (CVE-2010-1248)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel Memory Corruption Vulnerability (CVE-2010-1249)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel EDG Memory Corruption Vulnerability (CVE-2010-1250)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel Record Stack Corruption Vulnerability (CVE-2010-1251)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel String Variable Vulnerability (CVE-2010-1252)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for	Yes

						Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Excel ADO Object Vulnerability (CVE-2010-1253)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes
Jun-10	**MS10-038**	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)	Mac Office Open XML Permissions Vulnerability (CVE-2010-1254)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office System 2007, Excel 2007, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac	Yes
Jun-10	**MS10-039**	Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2028554)	toStaticHTML Information Disclosure Vulnerability (CVE-2010-1257)	Important	Elevation of Privileges	InfoPath 2003, InfoPath 2007, Office SharePoint Server 2007, Windows SharePoint Services 3.0	No
Jun-10	**MS10-039**	Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (202854)	SharePoint Help Page Denial of Service Vulnerability (CVE-2010-1264)	Important	Elevation of Privileges	InfoPath 2003, InfoPath 2007, Office SharePoint Server 2007, Windows SharePoint Services 3.0	No
Jun-10	**MS10-040**	Vulnerability in Internet Information Services Could Allow Remote Code Execution (982666)	IIS Authentication Memory Corruption Vulnerability (CVE-2010-1256)	Important	Remote Code Execution	Windows Server 2003 Internet Information Services 6.0, Internet Information Services 7.0, Internet Information Services 7.5, Windows Vista, Windows Server 2008, Windows 7	No
Jun-10	**MS10-041**	Vulnerability in Microsoft .NET Framework Could Allow Tampering (981343)	XML Signature HMAC Truncation Authentication Bypass Vulnerability (CVE-2009-0217)	Important	Tampering	Windows 2000 Server, Windows 2000, .Net Framework 1.1, .Net Framework 2.0, Windows XP, Net Framework 1.0, Net Framework 3.5, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	No
Jul-10	**MS10-042**	Vulnerability in Help and Support Center Could Allow Remote Code Execution (2229593)	Help Center URL Validation Vulnerability (CVE-2010-1885)	Critical	Remote Code Execution	Windows XP, Windows Server 2003	Yes
Jul-10	**MS10-043**	Vulnerability in Canonical Display Driver Could Allow Remote Code Execution (2032276)	Canonical Display Driver Integer Overflow Vulnerability (CVE-2009-3678)	Critical	Remote Code Execution	Windows 7, Windows Embedded Standard 7, Windows Server 2008	No

Jul-10	**MS10-044**	Vulnerabilities in Microsoft Office Access ActiveX Controls Could Allow Remote Code Execution (982335)	Access ActiveX Control Vulnerability (CVE-2010-0814)	Critical	Remote Code Execution	Office 2003, Access 2003, Office System 2007, Access 2007	Yes
Jul-10	**MS10-044**	Vulnerabilities in Microsoft Office Access ActiveX Controls Could Allow Remote Code Execution (982335)	ACCWIZ.dll Uninitialized Variable Vulnerability (CVE-2010-1881)	Critical	Remote Code Execution	Office 2003, Access 2003, Office System 2007, Access 2007	Yes
Jul-10	**MS10-045**	Vulnerability in Microsoft Office Outlook Could Allow Remote Code Execution (978212)	Microsoft Outlook SMB Attachment Vulnerability (CVE-2010-0266)	Important	Remote Code Execution	Office XP, Outlook 2002, Office 2003, Outlook 2003, Office System 2007, Outlook 2007	Yes
Aug-10	**MS10-046**	Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)	Shortcut Icon Loading Vulnerability (CVE-2010-2568)	Critical	Remote Code Execution	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Aug-10	**MS10-047**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)	Windows Kernel Data Initialization Vulnerability (CVE-2010-1888)	Important	Elevation of Privilege	Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-047**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)	Windows Kernel Double Free Vulnerability (CVE-2010-1889)	Important	Elevation of Privilege	Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-047**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)	Windows Kernel Improper Validation Vulnerability (CVE-2010-1890)	Important	Elevation of Privilege	Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-048**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)	Win32k Bounds Checking Vulnerability (CVE-2010-1887)	Important	Elevation of Privilege	Windows XP Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-048**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)	Win32k Pool Overflow Vulnerability (CVE-2010-1895)	Important	Elevation of Privilege	Windows XP Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-048**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)	Win32k User Input Validation Vulnerability (CVE-2010-1896)	Important	Elevation of Privilege	Windows XP Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-048**	Vulnerabilities in Windows Kernel-Mode	Win32k Window Creation	Important	Elevation of Privilege	Windows XP Windows Server 2003, Windows Vista,	No

		Drivers Could Allow Elevation of Privilege (2160329)	Vulnerability (CVE-2010-1897)			Windows Server 2008, Windows 7, Windows Server 2008	
Aug-10	**MS10-049**	Vulnerabilities in SChannel could allow Remote Code Execution (980436)	TLS/SSL Renegotiation Vulnerability (CVE-2009-3555)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-049**	Vulnerabilities in SChannel could allow Remote Code Execution (980436)	SChannel Malformed Certificare Request Remote Code Execution Vulnerability (CVE-2010-2566)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-050**	Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (981997)	Movie Maker Memory Corruption Vulnerability (CVE-2010-2564)	Important	Remote Code Execution	Windows XP, Windows Vista,	Yes
Aug-10	**MS10-051**	Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2079403)	Msxml2.XMLHTTP.3.0 Response Handling Memory Corruption CVE-2010-2561	Critical	Remote Code Execution	Windows XP, Microsoft XML Core Services 3.0, Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	No
Aug-10	**MS10-052**	Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (2115168)	MPEG Layer-3 Audio Decoder Buffer Overflow Vulnerability (CVE-2010-1882)	Critical	Remote Code Execution	Windows Server 2003, Windows XP	Yes
Aug-10	**MS10-053**	Cumulative Security Update for Internet Explorer (2183461)	Event Handler Cross-Domain Vulnerability - CVE-2010-1258	Critical	Remote Code Execution	Internet Explorer 6.0 Windows Server 2003, Windows XP, Internet Explorer 7, Windows XP Professional 64-Bit Edition, Windows Vista Windows Server 2008, Internet Explorer 8	Yes
Aug-10	**MS10-053**	Cumulative Security Update for Internet Explorer (2183461)	Uninitialized Memory Corruption Vulnerability - CVE-2010-2556	Critical	Remote Code Execution	Internet Explorer 6.0 Windows Server 2003, Windows XP, Internet Explorer 7, Windows XP Professional 64-Bit Edition, Windows Vista Windows Server 2008, Internet Explorer 8	Yes
Aug-10	**MS10-053**	Cumulative Security Update for Internet Explorer (2183461)	Uninitialized Memory Corruption Vulnerability - CVE-2010-2557	Critical	Remote Code Execution	Internet Explorer 6.0 Windows Server 2003, Windows XP, Internet Explorer 7, Windows XP Professional 64-Bit Edition, Windows Vista Windows Server 2008, Internet Explorer 8	Yes
Aug-10	**MS10-053**	Cumulative Security Update for Internet Explorer (2183461)	Race Condition Memory Corruption Vulnerability - CVE-2010-2558	Critical	Remote Code Execution	Internet Explorer 6.0 Windows Server 2003, Windows XP, Internet Explorer 7, Windows XP Professional 64-Bit Edition, Windows Vista Windows	Yes

						Server 2008, Internet Explorer 8	
Aug-10	**MS10-053**	Cumulative Security Update for Internet Explorer (2183461)	Uninitialized Memory Corruption Vulnerability - CVE-2010-2559	Critical	Remote Code Execution	Internet Explorer 6.0 Windows Server 2003, Windows XP, Internet Explorer 7, Windows XP Professional 64-Bit Edition, Windows Vista Windows Server 2008, Internet Explorer 8	Yes
Aug-10	**MS10-053**	Cumulative Security Update for Internet Explorer (2183461)	HTML Layout Memory Corruption Vulnerability - CVE-2010-2560	Critical	Remote Code Execution	Internet Explorer 6.0 Windows Server 2003, Windows XP, Internet Explorer 7, Windows XP Professional 64-Bit Edition, Windows Vista Windows Server 2008, Internet Explorer 8	Yes
Aug-10	**MS10-054**	Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	SMB Pool Overflow Vulnerability (CVE-2010-2550)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-054**	Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	SMB Stack Exhaustion Vulnerability (CVE-2010-2552)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-055**	Vulnerability in Cinepak Codec Could Allow Remote Code Execution (982665)	Cinepak Codec Decompression Vulnerability (CVE-2010-2553)	Critical	Remote Code Execution	Windows XP, Windows Vista, Windows 7	Yes
Aug-10	**MS10-056**	Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638)	Word Record Parsing Vulnerability (CVE-2010-1900)	Critical	Remote Code Execution	Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Open XML File Format Converter for Mac, Office XP, Word 2002, Office 2003, Word 2003, Office System 2007, Word 2007, Office 2004 for Macintosh, Word Viewer 2003, Works 9	Yes
Aug-10	**MS10-056**	Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638)	Word RTF Parsing Engine Memory Corruption Vulnerability (CVE-2010-1901)	Critical	Remote Code Execution	Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Open XML File Format Converter for Mac, Office XP, Word 2002, Office 2003, Word 2003, Office System 2007, Word 2007, Office 2004 for Macintosh, Word Viewer 2003, Works 9	Yes
Aug-10	**MS10-056**	Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638)	Word RTF Parsing Buffer Overflow Vulnerability (CVE-2010-1902)	Critical	Remote Code Execution	Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Open XML File Format Converter for Mac, Office XP, Word 2002,	Yes

						Office 2003, Word 2003, Office System 2007, Word 2007, Office 2004 for Macintosh, Word Viewer 2003, Works 9	
Aug-10	**MS10-056**	Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638)	Word HTML Linked Objects Memory Corruption Vulnerability (CVE-2010-1903)	Critical	Remote Code Execution	Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Open XML File Format Converter for Mac, Office XP, Word 2002, Office 2003, Word 2003, Office System 2007, Word 2007, Office 2004 for Macintosh, Word Viewer 2003, Works 9	Yes
Aug-10	**MS10-057**	Vulnerability in Microsoft Office Excel Could Allow Remote Code Execution (2269707)	Excel Memory Corruption Vulnerability (CVE-2010-2562)	Important	Remote Code Execution	Office XP, Excel 2002, Office 2003, Excel 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Open XML File Format Converter for Mac	Yes
Aug-10	**MS10-058**	Vulnerabilities in TCP/IP could cause Elevation of Privilege (978886)	IPv6 Memory Corruption Vulnerability (CVE-2010-1892)	Important	Elevation of Privilege	Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-058**	Vulnerabilities in TCP/IP could cause Elevation of Privilege (978886)	Integer Overflow in Windows Networking Vulnerability (CVE-2010-1893)	Important	Elevation of Privilege	Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-059**	Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege	Tracing Registry Key ACL Vulnerability (CVE-2010-2554)	Important	Elevation of Privilege	Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-059**	Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege	Tracing Memory Corruption Vulnerability (CVE-2010-2555)	Important	Elevation of Privilege	Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-060**	Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906)	Microsoft Silverlight Memory Corruption Vulnerability (CVE-2010-0019)	Critical	Remote Code Execution	Windows XP, .Net Framework 3.5, .Net Framework 2.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, .NET Framework 3.5.1, Windows 7, Microsoft Silverlight 2.0, Microsoft Silverlight 3.0	Yes
Aug-10	**MS10-060**	Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906)	Microsoft Silverlight and Microsoft .NET Framework CLR Virtual Method Delegate Vulnerability (CVE-2010-1898)	Critical	Remote Code Execution	Windows XP, .Net Framework 3.5, .Net Framework 2.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, .NET Framework 3.5.1, Windows 7, Microsoft Silverlight 2.0, Microsoft Silverlight 3.0	Yes
Sep-10	**MS10-061**	Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290)	Print Spooler Service Impersonation Vulnerability	Critical	Remote Code Execution	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	No

			(CVE-2010-2729)				
Sep-10	**MS10-062**	Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution (975558)	MPEG-4 Codec Vulnerability (CVE-2010-0818)	Critical	Remote Code Execution	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008,	Yes
Sep-10	**MS10-063**	Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (2320113)	Uniscribe Font Parsing Engine Memory Corruption Vulnerability (CVE-2010-2738)	Critical	Remote Code Execution	Windows XP Windows Server 2003, Windows Vista, Windows Server 2008, Office XP, Office 2003, Office System 2007	Yes
Sep-10	**MS10-064**	Vulnerability in Microsoft Outlook Could Allow Remote Code Execution (2315011)	Heap Based Buffer Overflow in Outlook Vulnerability (CVE-2010-2728)	Critical	Remote Code Execution	Office 2003, Outlook 2003, Office XP, Outlook 2002, Office System 2007, Outlook 2007	Yes
Sep-10	**MS10-065**	Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960)	IIS Repeated Parameter Request Denial of Service Vulnerability (CVE-2010-1899)	Important	Remote Code Execution	Windows XP, Internet Information Services 5.1, Internet Information Services 6.0, Windows Server 2003, Windows Vista, Internet Information Services 7.0, Windows Server 2008, Windows 7 for 32-Bit Systems, Internet Information Services 7.5,	No
Sep-10	**MS10-065**	Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960)	Request Header Buffer Overflow Vulnerability (CVE-2010-2730)	Important	Remote Code Execution	Windows XP, Internet Information Services 5.1, Internet Information Services 6.0, Windows Server 2003, Windows Vista, Internet Information Services 7.0, Windows Server 2008, Windows 7 for 32-Bit Systems, Internet Information Services 7.5,	No
Sep-10	**MS10-066**	Vulnerability in Remote Procedure Call Could Allow Remote Code Execution (982802)	RPC Memory Corruption Vulnerability (CVE-2010-2567)	Important	Remote Code Execution	Windows Server 2003, Windows XP	Yes
Sep-10	**MS10-067**	Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2259922)	WordPad Word 97 Text Converter Memory Corruption Vulnerability (CVE-2010-2563)	Important	Remote Code Execution	Windows Server 2003, Windows XP	Yes
Sep-10	**MS10-068**	Vulnerability in Local Security Authority Subsystem Service Could Allow Elevation of Privilege (983539)	LSASS Heap Overflow Vulnerabilit (CVE-2010-0820)	Important	Elevation of Privilege	Windows Server 2003, Windows Server 2008, Windows XP, Windows 7, Windows Server 2008	No
Sep-10	**MS10-069**	Vulnerability in Windows Client/Server Runtime Subsystem Could Allow Elevation of Privilege (2121546)	CSRSS Local Elevation of Privilege Vulnerability - CVE-2010-1891	Important	Elevation of Privilege	Windows Server 2003, Windows XP	No

Sep-10	**MS10-070**	Vulnerability in ASP.NET Could Allow Information Disclosure (2418042)	ASP.NET Padding Oracle Vulnerability (CVE-2010-3332)	Important	Information Disclosure	Windows XP, .Net Framework 1.1, Windows Server 2003, Windows Vista, .Net Framework 3.5, Windows Server 2008, .NET Framework 3.5.1, Windows 7, .Net Framework 4.0,	No
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	HTML Sanitization Vulnerability (CVE-2010-3243)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	HTML Sanitization Vulnerability (CVE-2010-3324)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	Uninitialized Memory Corruption Vulnerability (CVE-2010-3326)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	Uninitialized Memory Corruption Vulnerability (CVE-2010-3328)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	Uninitialized Memory Corruption Vulnerability (CVE-2010-3329)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	Cross-Domain Information Disclosure Vulnerability (CVE-2010-3330)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	Uninitialized Memory Corruption Vulnerability (CVE-2010-3331)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-10	**MS10-072**	Vulnerabilities in SafeHTML Could Allow Information Disclosure (2412048)	HTML Sanitization Vulnerability (CVE-2010-3243)	Important	Information Disclosure	Office SharePoint Server 2007, Office SharePoint Server 2007 x64 Edition, Windows SharePoint Services 3.0, Microsoft SharePoint Foundation 2010, Office Groove Server 2010, Office Web Applications	No

Oct-10	**MS10-072**	Vulnerabilities in SafeHTML Could Allow Information Disclosure (2412048)	HTML Sanitization Vulnerability (CVE-2010-3324)	Important	Information Disclosure	Office SharePoint Server 2007, Office SharePoint Server 2007 x64 Edition, Windows SharePoint Services 3.0, Microsoft SharePoint Foundation 2010, Office Groove Server 2010, Office Web Applications	No
Oct-10	**MS10-073**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)	Win32k Keyboard Layout Vulnerability (CVE-2010-2743)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows Vista	No
Oct-10	**MS10-073**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)	Win32k Window Class Vulnerability (CVE-2010-2744)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows Vista	No
Oct-10	**MS10-074**	Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution (2387149)	Windows MFC Document Title Updating Buffer Overflow Vulnerability (CVE-2010-3227)	Moderate	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	Yes
Oct-10	**MS10-075**	Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution (2281679)	RTSP use after free vulnerability (CVE-2010-3225)	Critical	Remote Code Execution	Windows Vista, Windows 7	No
Oct-10	**MS10-076**	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132)	Embedded OpenType Font Integer Overflow Vulnerability (CVE-2010-1883)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows Server 2008 Windows 7	Yes
Oct-10	**MS10-077**	Vulnerability in .NET Framework Could Allow Remote Code Execution (2160841)	.NET Framework x64 JIT Compiler Vulnerability (CVE-2010-3228)	Critical	Remote Code Execution	.Net Framework 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Oct-10	**MS10-078**	Vulnerabilities in the OpenType Font (OTF) Format Driver Could Allow Elevation of Privilege (2279986)	OpenType Font Parsing Vulnerability (CVE-2010-2740)	Important	Elevation of Privilege	Windows Server 2003, Windows XP	No
Oct-10	**MS10-078**	Vulnerabilities in the OpenType Font (OTF) Format Driver Could Allow Elevation of Privilege (2279986)	OpenType Font Validation Vulnerability (CVE-2010-2741)	Important	Elevation of Privilege	Windows Server 2003, Windows XP	No
Oct-10	**MS10-079**	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	Word Uninitialized Pointer Vulnerability (CVE-2010-2747)	Important	Remote Code Execution	Word 2002, Office XP, Word 2003, Office 2003, Word 2007, Office System 2007, Open XML File Format Converter for Mac, Office 2004 for Macintosh, Office 2008 for Macintosh,	Yes

						Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Word Viewer, Office Web Applications, Word Web Application, Word 2010, Office 2010, Word 2010 x64, Office 2010 x64	
Oct-10	**MS10-079**	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	Word Boundary Check Vulnerability (CVE-2010-2748)	Important	Remote Code Execution	Word 2002, Office XP, Word 2003, Office 2003, Word 2007, Office System 2007, Open XML File Format Converter for Mac, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Word Viewer, Office Web Applications, Word Web Application, Word 2010, Office 2010, Word 2010 x64, Office 2010 x64	Yes
Oct-10	**MS10-079**	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	Word Index Vulnerability (CVE-2010-2750)	Important	Remote Code Execution	Word 2002, Office XP, Word 2003, Office 2003, Word 2007, Office System 2007, Open XML File Format Converter for Mac, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Word Viewer, Office Web Applications, Word Web Application, Word 2010, Office 2010, Word 2010 x64, Office 2010 x64	Yes
Oct-10	**MS10-079**	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	Word Stack Overflow Vulnerability (CVE-2010-3214)	Important	Remote Code Execution	Word 2002, Office XP, Word 2003, Office 2003, Word 2007, Office System 2007, Open XML File Format Converter for Mac, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Word Viewer, Office Web Applications, Word Web Application, Word 2010, Office 2010, Word 2010 x64, Office 2010 x64	Yes
Oct-10	**MS10-079**	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	Word Return Value Vulnerability (CVE-2010-3215)	Important	Remote Code Execution	Word 2002, Office XP, Word 2003, Office 2003, Word 2007, Office System 2007, Open XML File Format Converter for Mac, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft	Yes

						Office Word Viewer, Office Web Applications, Word Web Application, Word 2010, Office 2010, Word 2010 x64, Office 2010 x64	
Oct-10	**MS10-079**	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	Word Bookmarks Vulnerability (CVE-2010-3216)	Important	Remote Code Execution	Word 2002, Office XP, Word 2003, Office 2003, Word 2007, Office System 2007, Open XML File Format Converter for Mac, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Word Viewer, Office Web Applications, Word Web Application, Word 2010, Office 2010, Word 2010 x64, Office 2010 x64	Yes
Oct-10	**MS10-079**	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	Word Pointer Vulnerability (CVE-2010-3217)	Important	Remote Code Execution	Word 2002, Office XP, Word 2003, Office 2003, Word 2007, Office System 2007, Open XML File Format Converter for Mac, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Word Viewer, Office Web Applications, Word Web Application, Word 2010, Office 2010, Word 2010 x64, Office 2010 x64	Yes
Oct-10	**MS10-079**	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	Word Heap Overflow Vulnerability (CVE-2010-3218)	Important	Remote Code Execution	Word 2002, Office XP, Word 2003, Office 2003, Word 2007, Office System 2007, Open XML File Format Converter for Mac, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Word Viewer, Office Web Applications, Word Web Application, Word 2010, Office 2010, Word 2010 x64, Office 2010 x64	Yes
Oct-10	**MS10-079**	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	Word Index Parsing Vulnerability (CVE-2010-3219)	Important	Remote Code Execution	Word 2002, Office XP, Word 2003, Office 2003, Word 2007, Office System 2007, Open XML File Format Converter for Mac, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Word Viewer, Office Web Applications, Word Web Application, Word 2010, Office 2010, Word 2010 x64,	Yes

						Office 2010 x64	
Oct-10	**MS10-079**	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	Word Parsing Vulnerability (CVE-2010-3220)	Important	Remote Code Execution	Word 2002, Office XP, Word 2003, Office 2003, Word 2007, Office System 2007, Open XML File Format Converter for Mac, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Word Viewer, Office Web Applications, Word Web Application, Word 2010, Office 2010, Word 2010 x64, Office 2010 x64	Yes
Oct-10	**MS10-079**	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)	Word Parsing Vulnerability (CVE-2010-3221)	Important	Remote Code Execution	Word 2002, Office XP, Word 2003, Office 2003, Word 2007, Office System 2007, Open XML File Format Converter for Mac, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Word Viewer, Office Web Applications, Word Web Application, Word 2010, Office 2010, Word 2010 x64, Office 2010 x64	Yes
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Excel Record Parsing Integer Overflow Vulnerability (CVE-2010-3230)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	Yes
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Excel Record Parsing Memory Corruption Vulnerability (CVE-2010-3231)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	Yes
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Excel File Format Parsing Vulnerability (CVE-2010-3232)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office	Yes

						System 2007	
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Lotus 1-2-3 Workbook Parsing Vulnerability (CVE-2010-3233)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	Yes
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Formula Substream Memory Corruption Vulnerability (CVE-2010-3234)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	Yes
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Formula Biff Record Vulnerability (CVE-2010-3235)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	Yes
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Out Of Bounds Array Vulnerability (CVE-2010-3236)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	Yes
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Merge Cell Record Pointer Vulnerability (CVE-2010-3237)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	Yes
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Negative Future Function Vulnerability (CVE-2010-3238)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007	Yes

						File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Extra Out of Boundary Record Parsing Vulnerability (CVE-2010-3239)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	Yes
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Real Time Data Array Record Vulnerability (CVE-2010-3240)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	Yes
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Out-of-Bounds Memory Write in Parsing Vulnerability (CVE-2010-3241)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	Yes
Oct-10	**MS10-080**	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (2293211)	Ghost Record Type Parsing Vulnerability (CVE-2010-3242)	Important	Remote Code Execution	Excel 2002, Office XP, Excel 2003, Office 2003, Office 2004 for Macintosh, Office 2008 for Macintosh, Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats, Microsoft Office Excel Viewer, Open XML File Format Converter for Mac, Excel 2007, Office System 2007	Yes
Oct-10	**MS10-081**	Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2296011)	Comctl32 Heap Overflow Vulnerability (CVE-2010-2746)	Important	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	Yes
Oct-10	**MS10-082**	Vulnerability in Windows Media Player Could Allow Remote Code Execution (2378111)	Windows Media Player Memory Corruption Vulnerability (CVE-2010-2745)	Important	Remote Code Execution	Windows Media Player 9.0, Windows XP Windows Media Player 10, Windows Media Player 11, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Oct-	**MS10-083**	Vulnerability in COM	COM Validation	Important	Remote Code	Windows XP Windows	Yes

10		Validation in Windows Shell and WordPad Could Allow Remote Code Execution (2405882)	Vulnerability (CVE-2010-1263)		Execution	Server 2003, Windows Server 2008, Windows Vista, Windows 7,	
Oct-10	**MS10-084**	Vulnerability in Windows Local Procedure Call Could Cause Elevation of Privilege (2360937)	LPC Message Buffer Overrun Vulnerability (CVE-2010-3222)	Important	Elevation of Privileges	Windows Server 2003, Windows XP	No
Oct-10	**MS10-085**	Vulnerability in SChannel Could Allow Denial of Service (2207566)	TLSv1 Denial of Service Vulnerability (CVE-2010-3229)	Important	Denial of Service	Windows Server 2008, Windows Vista, Windows 7	No
Oct-10	**MS10-086**	Vulnerability in Windows Shared Cluster Disks Could Allow Tampering (2294255)	Permissions on New Cluster Disks Vulnerability (CVE-2010-3223)	Moderate	Tampering	Windows Server 2008	No
Nov-10	**MS10- 087**	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930)	PowerPoint Integer Underflow Causes Heap Corruption Vulnerability (CVE-2010-2573)	Critical	Remote Code Execution	Office 2003, Office 2004 for Macintosh, Office System 2007, Office 2008 for Macintosh, Office XP, Open XML File Format Converter for Mac, Office 2011 for Mac, Office 2010, Office 2010 x64	Yes
Nov-10	**MS10- 087**	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930)	RTF Stack Buffer Overflow Vulnerability (CVE-2010-3333)	Critical	Remote Code Execution	Office 2003, Office 2004 for Macintosh, Office System 2007, Office 2008 for Macintosh, Office XP, Open XML File Format Converter for Mac, Office 2011 for Mac, Office 2010, Office 2010 x64	Yes
Nov-10	**MS10- 087**	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930)	Office Art Drawing Records Vulnerability (CVE-2010-3334)	Critical	Remote Code Execution	Office 2003, Office 2004 for Macintosh, Office System 2007, Office 2008 for Macintosh, Office XP, Open XML File Format Converter for Mac, Office 2011 for Mac, Office 2010, Office 2010 x64	Yes
Nov-10	**MS10- 087**	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930)	Drawing Exception Handling Vulnerability (CVE-2010-3335)	Critical	Remote Code Execution	Office 2003, Office 2004 for Macintosh, Office System 2007, Office 2008 for Macintosh, Office XP, Open XML File Format Converter for Mac, Office 2011 for Mac, Office 2010, Office 2010 x64	Yes
Nov-10	**MS10- 087**	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930)	MSO Large SPID Read AV Vulnerability (CVE-2010-3336)	Critical	Remote Code Execution	Office 2003, Office 2004 for Macintosh, Office System 2007, Office 2008 for Macintosh, Office XP, Open XML File Format Converter for Mac, Office 2011 for Mac, Office 2010, Office 2010 x64	Yes
Nov-10	**MS10- 087**	Vulnerabilities in	Insecure Library Loading	Critical	Remote Code Execution	Office 2003, Office 2004 for Macintosh, Office System	Yes

		Microsoft Office Could Allow Remote Code Execution (2423930)	Vulnerability (CVE-2010-3337)			2007, Office 2008 for Macintosh, Office XP, Open XML File Format Converter for Mac, Office 2011 for Mac, Office 2010, Office 2010 x64	
Nov-10	**MS10- 088**	Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2293386)	PowerPoint Parsing Buffer Overflow Vulnerability (CVE-2010-2572)	Important	Remote Code Execution	Office 2004 for Macintosh, PowerPoint 2002, Office XP, Office 2003, PowerPoint 2003, PowerPoint 2007 Viewer	Yes
Nov-10	**MS10- 088**	Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2293386)	PowerPoint Integer Underflow Causes Heap Corruption Vulnerability (CVE-2010-2573)	Important	Remote Code Execution	Office 2004 for Macintosh, PowerPoint 2002, Office XP, Office 2003, PowerPoint 2003, PowerPoint 2007 Viewer	Yes
Nov-10	**MS10-089**	Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Elevation of Privilege (2316074)	UAG Redirection Spoofing Vulnerability (CVE-2010-2732)	Important	Elevation of Privilege	Forefront UAG 2010	No
Nov-10	**MS10-089**	Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Elevation of Privilege (2316074)	UAG XSS Allows EOP Vulnerability (CVE-2010-2733)	Important	Elevation of Privilege	Forefront UAG 2010	No
Nov-10	**MS10-089**	Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Elevation of Privilege (2316074)	XXS Issue on UAG Mobile Portal Websie in Forefront Unified Access Gateway Vulnerability (CVE-2010-2734)	Important	Elevation of Privilege	Forefront UAG 2010	No
Nov-10	**MS10-089**	Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Elevation of Privilege (2316074)	XSS in Signurl.asp Vulnerability (CVE-2010-3936)	Important	Elevation of Privilege	Forefront UAG 2010	No
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	HTML Object Memory Corruption Vulnerability (CVE-2010-3340)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	HTML Object Memory Corruption Vulnerability (CVE-2010-3343)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	HTML Element Memory Corruption Vulnerability (CVE-2010-3345)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-090**	Cumulative Security Update for Internet	HTML Element Memory Corruption	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet	Yes

		Explorer (2416400)	Vulnerability (CVE-2010-3346)			Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	Cross-Domain Information Disclosure Vulnerability (CVE-2010-3348)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	Cross-Domain Information Disclosure Vulnerability (CVE-2010-3348)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	Uninitialized Memory Corruption Vulnerability (CVE-2010-3962)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-091**	Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution	OpenType Font Index Vulnerability (CVE-2010-3956)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10-091**	Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution	OpenType Font Double Free Vulnerability (CVE-2010-3957)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10-091**	Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution	OpenType CMAP Table Vulnerability (CVE-2010-3959)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10-092**	Vulnerability in Task Scheduler Could Allow Elevation of Privilege (2305420)	Task Scheduler Vulnerability (CVE-2010-3338)	Important	Elevation of Privilege	Windows Vista, Windows Server 2008, Windows 7	No
Dec-10	**MS10-093**	Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (2424434)	Insecure Library Loading Vulnerability (CVE-2010-3967)	Important	Remote Code Execution	Windows Vista	No
Dec-10	**MS10-094**	Vulnerability in Windows Media Encoder Could Allow Remote Code Execution (2447961)	Insecure Library Loading Vulnerability (CVE-2010-3965)	Important	Remote Code Execution	Windows XP, Windows Media Encoder 9 Series, Windows Server 2003, Windows Vista, Windows Server 2008,	No
Dec-10	**MS10-095**	Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2385678)	BranchCache Insecure Library Loading Vulnerability (CVE-2010-3966)	Important	Remote Code Execution	Windows 7, Windows Server 2008	No

Dec-10	**MS10-096**	Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089)	Insecure Library Loading Vulnerability (CVE-2010-3147)	Important	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10-097**	Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution (2443105)	Internet Connection Signup Wizard Insecure Library Loading Vulnerability (CVE-2010-3144)	Important	Remote Code Execution	Windows Server 2003, Windows XP	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Win 32k Buffer Overflow Vulnerability (CVE-2010-3939)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Win32k PFE Pointer Double Free Vulnerability (CVE-2010-3940)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Windows Kernel Double Free Vulnerability (CVE-2010-3941)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Windows Kernel WriteAV Vulnerability (CVE-2010-3942)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Windows Kernel Cursor Linking Vulnerability (CVE-2010-3943)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Windows Kernel Memory Corruption Vulnerability (CVE-2010-3944)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Windows Kernel Memory Corruption Vulnerability (CVE-2010-3944)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10-099**	Vulnerability in Routing and Remote Access Could Allow Elevation of Privilege	Kernel NDProxy Buffer Overflow Vulnerability (CVE-2010-3963)	Important	Elevation of Privilege	Windows Server 2003, Windows XP	No

		(2440591)					
Dec-10	**MS10- 100**	Vulnerability in Consent User Interface Could Allow Elevation of Privilege (2442962)	Consent UI Impersonation Vulnerability (CVE-2010-3961)	Important	Elevation of Privilege	Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 101**	Vulnerability in Windows Netlogon Service Could Allow Denial of Service (2207559)	Netlogon RPC Null dereference DOS Vulnerability (CVE-2010-2742)	Important	Denial of Service	Windows Server 2003, Windows Server 2008,	No
Dec-10	**MS10- 102**	Vulnerability in Hyper-V Could Allow Denial of Service (2345316)	Hyper-V VMBus vulnerability (CVE-2010-3960)	Important	Denial of Service	Windows Server 2008	No
Dec-10	**MS10- 103**	Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2292970)	Size Value Heap Corruption in pubconv.dll Vulnerability (CVE-2010-2569)	Important	Remote Code Execution	Office XP, Publisher 2002, Office 2003, Publisher 2003, Office System 2007, Publisher 2007, Office 2010, Publisher 2010, Office 2010 x64	Yes
Dec-10	**MS10- 103**	Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2292970)	Heap Overrun in pubconv.dll Vulnerability (CVE-2010-2570)	Important	Remote Code Execution	Office XP, Publisher 2002, Office 2003, Publisher 2003, Office System 2007, Publisher 2007, Office 2010, Publisher 2010, Office 2010 x64	Yes
Dec-10	**MS10- 103**	Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2292970)	Memory Corruption Due To Invalid Index Into Array in Pubconv.dll Vulnerability (CVE-2010-2571)	Important	Remote Code Execution	Office XP, Publisher 2002, Office 2003, Publisher 2003, Office System 2007, Publisher 2007, Office 2010, Publisher 2010, Office 2010 x64	Yes
Dec-10	**MS10- 103**	Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2292970)	Microsoft Publisher Memory Corruption Vulnerability (CVE-2010-3954)	Important	Remote Code Execution	Office XP, Publisher 2002, Office 2003, Publisher 2003, Office System 2007, Publisher 2007, Office 2010, Publisher 2010, Office 2010 x64	Yes
Dec-10	**MS10- 103**	Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2292970)	Array Indexing Memory Corruption Vulnerability (CVE-2010-3955)	Important	Remote Code Execution	Office XP, Publisher 2002, Office 2003, Publisher 2003, Office System 2007, Publisher 2007, Office 2010, Publisher 2010, Office 2010 x64	Yes
Dec-10	**MS10- 104**	Vulnerability in Microsoft SharePoint Could Allow Remote Code Execution (2455005)	Malformed Request Code Execution Vulnerability (CVE-2010-3964)	Important	Remote Code Execution	Office SharePoint Server 2007, Office SharePoint Server 2007 x64 Edition	No
Dec-10	**MS10- 105**	Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)	CGM Image Converter Buffer Overrun Vulnerability (CVE-2010-3945)	Important	Remote Code Execution	Office 2003, Office XP, Works 9, Microsoft Office Converter Pack	Yes
Dec-	**MS10- 105**	Vulnerabilities in	PICT Image	Important	Remote Code	Office 2003, Office XP,	Yes

10		Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)	Converter Integer Overflow Vulnerability (CVE-2010-3946)		Execution	Works 9, Microsoft Office Converter Pack	
Dec-10	**MS10- 105**	Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)	TIFF Image Converter Heap Overflow Vulnerability (CVE-2010-3947)	Important	Remote Code Execution	Office 2003, Office XP, Works 9, Microsoft Office Converter Pack	Yes
Dec-10	**MS10- 105**	Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)	TIFF Image Converter Buffer Overflow Vulnerability (CVE-2010-3949)	Important	Remote Code Execution	Office 2003, Office XP, Works 9, Microsoft Office Converter Pack	Yes
Dec-10	**MS10- 105**	Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)	TIFF Image Converter Memory Corruption Vulnerability (CVE-2010-3950)	Important	Remote Code Execution	Office 2003, Office XP, Works 9, Microsoft Office Converter Pack	Yes
Dec-10	**MS10- 105**	Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)	FlashPix Image Converter Buffer Overflow Vulnerability (CVE-2010-3951)	Important	Remote Code Execution	Office 2003, Office XP, Works 9, Microsoft Office Converter Pack	Yes
Dec-10	**MS10- 105**	Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)	FlashPix Image Converter Heap Corruption Vulnerability (CVE-2010-3952)	Important	Remote Code Execution	Office 2003, Office XP, Works 9, Microsoft Office Converter Pack	Yes
Dec-10	**MS10- 106**	Vulnerability in Microsoft Exchange Server Could Allow Denial of Service (2407132)	Exchange Server Infinite Loop Vulnerability (CVE-2010-3937)	Moderate	Denial of Service	Exchange Server 2007	No

Appendix B- Windows 7 Vulnerabilities to Date

Date	Bulletin ID	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Oct-09	**MS09-056**	Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571)	Null Truncation in X.509 Common Name Vulnerability - CVE-2009-2510	Important	Spoofing	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	No
Oct-09	**MS09-056**	Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571)	Integer Overflow in X.509 Object Identifiers Vulnerability - CVE-2009-2511	Important	Spoofing	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	No
Oct-09	**MS09-056**	Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (974571)	Local Security Authority Subsystem Service Integer Overflow Vulnerability - CVE-2009-2524	Important	Spoofing	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	No
Dec-09	**MS09-072**	Cumulative Security Update for Internet Explorer (976325)	Uninitialized Memory Corruption Vulnerability - CVE-2009-3671	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-09	**MS09-072**	Cumulative Security Update for Internet Explorer (976325)	Uninitialized Memory Corruption Vulnerability - CVE-2009-3673	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-09	**MS09-072**	Cumulative Security Update for Internet Explorer (976325)	Uninitialized Memory Corruption Vulnerability - CVE-2009-3674	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Jan-10	**MS10-001**	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)	Microtype Express Compressed Fonts Integer Flaw in the LZCOMP Decompressor Vulnerability - CVE-2010-0018	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	Yes
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	XSS Filter Script Handling Vulnerability - CVE-2009-4074	Moderate	Information Disclosure	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No

Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	URL Validation Vulnerability - CVE-2010-0027	Moderate	Information Disclosure	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	Uninitialized Memory Corruption Vulnerability - CVE-2010-0244	Moderate	Information Disclosure	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	Uninitialized Memory Corruption Vulnerability - CVE-2010-0245	Moderate	Information Disclosure	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	Uninitialized Memory Corruption Vulnerability - CVE-2010-0246	Moderate	Information Disclosure	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	HTML Object Memory Corruption Vulnerability - CVE-2010-0248	Moderate	Information Disclosure	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Jan-10	**MS10-002**	Cumulative Security Update for Internet Explorer (978207)	HTML Object Memory Corruption Vulnerability - CVE-2010-0249	Moderate	Information Disclosure	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Feb-10	**MS10-006**	Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)	SMB Client Race Condition Vulnerability - CVE-2010-0017	Critical	Elevation of Privilege	Windows Vista, Windows Server 2008, Windows 7	No
Feb-10	**MS10-008**	Cumulative Security Update of ActiveX Kill Bits (978262)	Microsoft Data Analyzer ActiveX Control Vulnerability - CVE-2010-0252	Important	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	Yes
Feb-10	**MS10-013**	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935)	DirectShow Heap Overflow Vulnerability - CVE-2010-0250	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	Yes
Feb-10	**MS10-012**	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	SMB Pathname Overflow Vulnerability - CVE-2010-0020	Important	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Feb-10	**MS10-012**	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	SMB Memory Corruption Vulnerability - CVE-2010-0021	Important	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No

Feb-10	**MS10-012**	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	SMB Null Pointer Vulnerability - CVE-2010-0022	Important	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Feb-10	**MS10-012**	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	SMB NTLM Authentication Lack of Entropy Vulnerability - CVE-2010-0231	Important	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Feb-10	**MS10-015**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)	Windows Kernel Exception Handler Vulnerability - CVE-2010-0232	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Mar-10	**MS10-016**	Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (975561)	Movie Maker and Producer Buffer Overflow Vulnerability – CVE-2010-0265	Important	Remote Code Execution	Microsoft Office, Windows XP, Windows Vista, Windows 7	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	Uninitialized Memory Corruption Vulnerability (CVE-2010-0267)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	Post Encoding Information Disclosure Vulnerability (CVE-2010-0488)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	Uninitialized Memory Corruption Vulnerability (CVE-2010-0490)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	HTML Object Memory Corruption Vulnerability (CVE-2010-0491)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	HTML Object Memory Corruption Vulnerability	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer	Yes

			(CVE-2010-0492)			7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	HTML Element Cross-Domain Vulnerability (CVE-2010-0494)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	Memory Corruption Vulnerability (CVE-2010-0805)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	Uninitialized Memory Corruption Vulnerability (CVE-2010-0806)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Mar-10	**MS10-018**	Cumulative Security Update for Internet Explorer (980182)	HTML Rendering Memory Corruption Vulnerability (CVE-2010-0807)	Critical	Remote Code Execution	Internet Explorer 5.01, Windows 2000 Server, Windows 2000, Internet Explorer 6, Internet Explorer 7, Windows Server 2003 Windows XP, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7, Internet Explorer 8	Yes
Apr-10	**MS10-019**	Vulnerabilities in Windows Could Allow Remote Code Execution (981210)	WinVerify Trust Signature Validation Vulnerability-CVE-2010-0486	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Apr-10	**MS10-019**	Vulnerabilities in Windows Could Allow Remote Code Execution (981210)	Cabview Corruption Validation Vulnerability-CVE-2010-0487	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Apr-10	**MS10-020**	Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)	SMB Client Memory Allocation Vulnerability (CVE-2010-0269)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7 Windows Server 2008	No
Apr-10	**MS10-020**	Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)	SMB Client Transaction Vulnerability (CVE-2010-0270)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003 Windows Vista, Windows	No

						Server 2008, Windows 7 Windows Server 2008	
Apr-10	**MS10-020**	Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)	SMB Client Response Parsing Vulnerability (CVE-2010-0476)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7 Windows Server 2008	No
Apr-10	**MS10-020**	Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)	SMB Client Message Size Vulnerability (CVE-2010-0477)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Null Pointer Vulnerability(CVE-2010-0234)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Symbolic Link Value Vulnerability (CVE-2010-0235)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Memory Allocation Vulnerability (CVE-2010-0236)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Symbolic Link Creation Vulnerability (CVE-2010-0237)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Registry Key Vulnerability (CVE-2010-0238)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Virtual Path Parsing Vulnerability (CVE-2010-0481)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Malformed Image Vulnerability (CVE-2010-0482)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-021**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)	Windows Kernel Exception Handler Vulnerability (CVE-2010-0810)	Important	Elevation of Privileges	Windows 2000, Windows 2000 Server, Windows Server 2003, Windows Server 2008, Windows XP, Windows Vista, Windows 7 Windows Server 2008	No
Apr-10	**MS10-022**	Vulnerability in VBScript Scripting Engine Could Allow	VBScript Help Keypress Vulnerability –	Important	Remote Code Execution	Windows 2000 Server, Windows 2000, Windows XP, Windows Server 2003 Windows Vista, Windows	Yes

		Remote Code Execution (981169)	CVE-2010-0483			Server 2008, Windows 7	
May-10	**MS10-030**	Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)	Windows Mail Client Integer Overflow Vulnerability (CVE-2010-0816)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Outlook Express 5.5, Outlook Express 6, Windows XP, Windows Live Mail, Windows Mail, Windows Vista, Windows Server 2003, Windows Server 2008, Windows 7	Yes
Jun-10	**MS10-032**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)	Win32k Improper Data Validation Vulnerability (CVE-2010-0484)	Important	Elevation of Privilege	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	No
Jun-10	**MS10-032**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)	Win32k TrueType Font Parsing Vulnerability (CVE-2010-1255)	Important	Elevation of Privilege	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	No
Jun-10	**MS10-033**	Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)	Media Decompression Vulnerability (CVE-2010-1879)	Critical	Remote Code Execution	Windows Server 2003, Windows XP Windows 2000 Advanced Server, Windows 2000, Windows Media Encoder 9 Series, Windows Vista, Windows Server 2008 Windows 7	Yes
Jun-10	**MS10-033**	Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)	MJEP Media Decompression Vulnerability (CVE-2010-1880)	Critical	Remote Code Execution	Windows Server 2003, Windows XP Windows 2000 Advanced Server, Windows 2000, Windows Media Encoder 9 Series, Windows Vista, Windows Server 2008 Windows 7	Yes
Jun-10	**MS10-034**	Cumulative Security Update of ActiveX Kill Bits (980195)	Microsoft Data Analyzer ActiveX Control Vulnerability (CVE-2010-0252)	Critical	Active X Kill Bits	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	Yes
Jun-10	**MS10-034**	Cumulative Security Update of ActiveX Kill Bits (980195)	Microsoft internet Explorer 8 Developer Tools Vulnerability (CVE-2010-0811)	Critical	Active X Kill Bits	Windows 2000 Server, Windows 2000, Windows XP Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	Yes
Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	toStaticHTML Information Disclosure Vulnerability (CVE-2010-1257)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	Yes
Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	toStaticHTML Information Disclosure Vulnerability (CVE-2010-1257)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	Yes

Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	Uninitialized Memory Corruption Vulnerability (CVE-2010-1259)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	Yes
Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	HTML Element Memory Corruption Vulnerability (CVE-2010-1260)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	Yes
Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	Uninitialized Memory Corruption Vulnerability (CVE-2010-1261)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	Yes
Jun-10	**MS10-035**	Cumulative Security Update for Internet Explorer (982381)	Memory Corruption Vulnerability (CVE-2010-1262)	Critical	Remote Code Execution	Windows 2000 Server, Windows 2000, Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 7.0 Windows XP, Windows Server 2003, Windows Vista Windows Server 2008, Windows 7 Internet Explorer 8.0	Yes
Jun-10	**MS10-036**	Vulnerability in COM Validation in Microsoft Office Could Allow Remote Code Execution (983235)	COM Validation Vulnerability (CVE-2010-1263)	Important	Remote Code Execution	Office XP, Office 2003, Excel 2003, PowerPoint 2003, Publisher 2003, Visio 2003, Word 2003, Office System 2007, Excel 2007, PowerPoint 2007, Visio 2007, Word 2007, Publisher 2007	Yes
June-10	**MS10-037**	Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)	OpenType CFF Font Driver Memory Corruption Vulnerability (CVE-2010-0819)	Important	Elevation of Privilege	Windows 2000 Server, Windows 2000, Windows XP, Windows Vista, Windows Server 2003 Windows Server 2008, Windows 7	No
Jun-10	**MS10-040**	Vulnerability in Internet Information Services Could Allow Remote Code Execution (982666)	IIS Authentication Memory Corruption Vulnerability (CVE-2010-1256)	Important	Remote Code Execution	Windows Server 2003 Internet Information Services 6.0, Internet Information Services 7.0, Internet Information Services 7.5, Windows Vista, Windows Server 2008, Windows 7	No
Jun-10	**MS10-041**	Vulnerability in Microsoft .NET Framework Could Allow Tampering (981343)	XML Signature HMAC Truncation Authentication Bypass Vulnerability (CVE-2009-0217)	Important	Tampering	Windows 2000 Server, Windows 2000, .Net Framework 1.1, .Net Framework 2.0, Windows XP, Net Framework 1.0, Net Framework 3.5, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	No
Jul-	**MS10-043**	Vulnerability in	Canonical Display	Critical	Remote Code	Windows 7, Windows	No

10		Canonical Display Driver Could Allow Remote Code Execution (2032276)	Driver Integer Overflow Vulnerability (CVE-2009-3678)		Execution	Embedded Standard 7, Windows Server 2008	
Aug-10	**MS10-046**	Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)	Shortcut Icon Loading Vulnerability (CVE-2010-2568)	Critical	Remote Code Execution	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Aug-10	**MS10-047**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)	Windows Kernel Data Initialization Vulnerability (CVE-2010-1888)	Important	Elevation of Privilege	Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-047**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)	Windows Kernel Double Free Vulnerability (CVE-2010-1889)	Important	Elevation of Privilege	Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-047**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)	Windows Kernel Improper Validation Vulnerability (CVE-2010-1890)	Important	Elevation of Privilege	Windows XP, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-048**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)	Win32k Bounds Checking Vulnerability (CVE-2010-1887)	Important	Elevation of Privilege	Windows XP Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-048**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)	Win32k Pool Overflow Vulnerability (CVE-2010-1895)	Important	Elevation of Privilege	Windows XP Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-048**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)	Win32k User Input Validation Vulnerability (CVE-2010-1896)	Important	Elevation of Privilege	Windows XP Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-048**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)	Win32k Window Creation Vulnerability (CVE-2010-1897)	Important	Elevation of Privilege	Windows XP Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008	No
Aug-10	**MS10-049**	Vulnerabilities in SChannel could allow Remote Code Execution (980436)	TLS/SSL Renegotiation Vulnerability (CVE-2009-3555)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-049**	Vulnerabilities in SChannel could allow Remote Code Execution (980436)	SChannel Malformed Certificare Request Remote Code Execution Vulnerability (CVE-2010-2566)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No

Aug-10	**MS10-051**	Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2079403)	Msxml2.XMLHTTP.3.0 Response Handling Memory Corruption CVE-2010-2561	Critical	Remote Code Execution	Windows XP, Microsoft XML Core Services 3.0, Windows Server 2003 Windows Vista, Windows Server 2008, Windows 7	No
Aug-10	**MS10-054**	Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	SMB Pool Overflow Vulnerability (CVE-2010-2550)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-054**	Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)	SMB Stack Exhaustion Vulnerability (CVE-2010-2552)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-055**	Vulnerability in Cinepak Codec Could Allow Remote Code Execution (982665)	Cinepak Codec Decompression Vulnerability (CVE-2010-2553)	Critical	Remote Code Execution	Windows XP, Windows Vista, Windows 7	Yes
Aug-10	**MS10-058**	Vulnerabilities in TCP/IP could cause Elevation of Privilege (978886)	IPv6 Memory Corruption Vulnerability (CVE-2010-1892)	Important	Elevation of Privilege	Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-058**	Vulnerabilities in TCP/IP could cause Elevation of Privilege (978886)	Integer Overflow in Windows Networking Vulnerability (CVE-2010-1893)	Important	Elevation of Privilege	Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-059**	Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege	Tracing Registry Key ACL Vulnerability (CVE-2010-2554)	Important	Elevation of Privilege	Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-059**	Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege	Tracing Memory Corruption Vulnerability (CVE-2010-2555)	Important	Elevation of Privilege	Windows Server 2008, Windows Vista, Windows 7	No
Aug-10	**MS10-060**	Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906)	Microsoft Silverlight Memory Corruption Vulnerability (CVE-2010-0019)	Critical	Remote Code Execution	Windows XP, .Net Framework 3.5, .Net Framework 2.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, .NET Framework 3.5.1, Windows 7, Microsoft Silverlight 2.0, Microsoft Silverlight 3.0	Yes
Aug-10	**MS10-060**	Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906)	Microsoft Silverlight and Microsoft .NET Framework CLR Virtual Method Delegate Vulnerability (CVE-2010-1898)	Critical	Remote Code Execution	Windows XP, .Net Framework 3.5, .Net Framework 2.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, .NET Framework 3.5.1, Windows 7, Microsoft Silverlight 2.0, Microsoft Silverlight 3.0	Yes
Sep-10	**MS10-061**	Vulnerability in Print Spooler Service Could	Print Spooler Service	Critical	Remote Code Execution	Windows XP, Windows Server 2003, Windows Vista,	No

		Allow Remote Code Execution (2347290)	Impersonation Vulnerability (CVE-2010-2729)			Windows Server 2008, Windows 7	
Sep-10	**MS10-065**	Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960)	IIS Repeated Parameter Request Denial of Service Vulnerability (CVE-2010-1899)	Important	Remote Code Execution	Windows XP, Internet Information Services 5.1, Internet Information Services 6.0, Windows Server 2003, Windows Vista, Internet Information Services 7.0, Windows Server 2008, Windows 7 for 32-Bit Systems, Internet Information Services 7.5,	No
Sep-10	**MS10-065**	Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960)	Request Header Buffer Overflow Vulnerability (CVE-2010-2730)	Important	Remote Code Execution	Windows XP, Internet Information Services 5.1, Internet Information Services 6.0, Windows Server 2003, Windows Vista, Internet Information Services 7.0, Windows Server 2008, Windows 7 for 32-Bit Systems, Internet Information Services 7.5,	No
Sep-10	**MS10-068**	Vulnerability in Local Security Authority Subsystem Service Could Allow Elevation of Privilege (983539)	LSASS Heap Overflow Vulnerabilit (CVE-2010-0820)	Important	Elevation of Privilege	Windows Server 2003, Windows Server 2008, Windows XP, Windows 7, Windows Server 2008	No
Sep-10	**MS10-070**	Vulnerability in ASP.NET Could Allow Information Disclosure (2418042)	ASP.NET Padding Oracle Vulnerability (CVE-2010-3332)	Important	Information Disclosure	Windows XP, .Net Framework 1.1, Windows Server 2003, Windows Vista, .Net Framework 3.5, Windows Server 2008, .NET Framework 3.5.1, Windows 7, .Net Framework 4.0,	No
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	HTML Sanitization Vulnerability (CVE-2010-3243)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	HTML Sanitization Vulnerability (CVE-2010-3324)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	Uninitialized Memory Corruption Vulnerability (CVE-2010-3326)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	Uninitialized Memory Corruption Vulnerability (CVE-2010-3328)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-2010	**MS10-071**	Cumulative Security Update for Internet	Uninitialized Memory	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition,	Yes

		Explorer (2360131)	Corruption Vulnerability (CVE-2010-3329)			Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	Cross-Domain Information Disclosure Vulnerability (CVE-2010-3330)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-2010	**MS10-071**	Cumulative Security Update for Internet Explorer (2360131)	Uninitialized Memory Corruption Vulnerability (CVE-2010-3331)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8.0, Windows 7	Yes
Oct-10	**MS10-074**	Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution (2387149)	Windows MFC Document Title Updating Buffer Overflow Vulnerability (CVE-2010-3227)	Moderate	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	Yes
Oct-10	**MS10-075**	Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution (2281679)	RTSP use after free vulnerability (CVE-2010-3225)	Critical	Remote Code Execution	Windows Vista, Windows 7	No
Oct-10	**MS10-076**	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132)	Embedded OpenType Font Integer Overflow Vulnerability (CVE-2010-1883)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows Server 2008 Windows 7	Yes
Oct-10	**MS10-077**	Vulnerability in .NET Framework Could Allow Remote Code Execution (2160841)	.NET Framework x64 JIT Compiler Vulnerability (CVE-2010-3228)	Critical	Remote Code Execution	.Net Framework 4.0, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Oct-10	**MS10-081**	Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2296011)	Comctl32 Heap Overflow Vulnerability (CVE-2010-2746)	Important	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	Yes
Oct-10	**MS10-082**	Vulnerability in Windows Media Player Could Allow Remote Code Execution (2378111)	Windows Media Player Memory Corruption Vulnerability (CVE-2010-2745)	Important	Remote Code Execution	Windows Media Player 9.0, Windows XP Windows Media Player 10, Windows Media Player 11, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	Yes
Oct-10	**MS10-083**	Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution (2405882)	COM Validation Vulnerability (CVE-2010-1263)	Important	Remote Code Execution	Windows XP Windows Server 2003, Windows Server 2008, Windows Vista, Windows 7,	Yes
Oct-	**MS10-085**	Vulnerability in	TLSv1 Denial of	Important	Denial of Service	Windows Server 2008,	No

10		SChannel Could Allow Denial of Service (2207566)	Service Vulnerability (CVE-2010-3229)			Windows Vista, Windows 7	
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	HTML Object Memory Corruption Vulnerability (CVE-2010-3340)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	HTML Object Memory Corruption Vulnerability (CVE-2010-3343)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	HTML Element Memory Corruption Vulnerability (CVE-2010-3345)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	HTML Element Memory Corruption Vulnerability (CVE-2010-3346)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	Cross-Domain Information Disclosure Vulnerability (CVE-2010-3348)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	Cross-Domain Information Disclosure Vulnerability (CVE-2010-3348)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-090**	Cumulative Security Update for Internet Explorer (2416400)	Uninitialized Memory Corruption Vulnerability (CVE-2010-3962)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Windows 7	Yes
Dec-10	**MS10-091**	Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution	OpenType Font Index Vulnerability (CVE-2010-3956)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10-091**	Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution	OpenType Font Double Free Vulnerability (CVE-2010-3957)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10-091**	Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution	OpenType CMAP Table Vulnerability (CVE-2010-3959)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No

Dec-10	**MS10-092**	Vulnerability in Task Scheduler Could Allow Elevation of Privilege (2305420)	Task Scheduler Vulnerability (CVE-2010-3338)	Important	Elevation of Privilege	Windows Vista, Windows Server 2008, Windows 7	No
Dec-10	**MS10-095**	Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2385678)	BranchCache Insecure Library Loading Vulnerability (CVE-2010-3966)	Important	Remote Code Execution	Windows 7, Windows Server 2008	No
Dec-10	**MS10-096**	Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089)	Insecure Library Loading Vulnerability (CVE-2010-3147)	Important	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Win 32k Buffer Overflow Vulnerability (CVE-2010-3939)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Win32k PFE Pointer Double Free Vulnerability (CVE-2010-3940)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Windows Kernel Double Free Vulnerability (CVE-2010-3941)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Windows Kernel WriteAV Vulnerability (CVE-2010-3942)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Windows Kernel Cursor Linking Vulnerability (CVE-2010-3943)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Windows Kernel Memory Corruption Vulnerability (CVE-2010-3944)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-10	**MS10- 098**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)	Windows Kernel Memory Corruption Vulnerability (CVE-2010-3944)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Dec-	**MS10- 100**	Vulnerability in	Consent UI	Important	Elevation of	Windows Server 2008,	No

10		Consent User Interface Could Allow Elevation of Privilege (2442962)	Impersonation Vulnerability (CVE-2010-3961)		Privilege	Windows Vista, Windows 7	
Jan-11	**MS11- 001**	Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (2451910)	DSN Overflow Vulnerability (CVE-2011-0026)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Jan-11	**MS11- 001**	Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (2451910)	ADO Record Memory Vulnerability (CVE-2011-0027)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	Yes
Feb-11	**MS11- 003**	Cumulative Security Update for Internet Explorer (2416400)	CSS Memory Corruption Vulnerability (CVE-2010-3971)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8, Windows 7	Yes
Feb-11	**MS11- 003**	Cumulative Security Update for Internet Explorer (2416400)	Uninitialized Memory Corruption Vulnerability (CVE-2011-0035)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8, Windows 7	Yes
Feb-11	**MS11- 003**	Cumulative Security Update for Internet Explorer (2416400)	Uninitialized Memory Corruption Vulnerability (CVE-2011-0036)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8, Windows 7	Yes
Feb-11	**MS11- 003**	Cumulative Security Update for Internet Explorer (2416400)	Internet Explorer Insecure Library Loading Vulnerability (CVE-2011-0038)	Critical	Remote Code Execution	Internet Explorer 6.0, Windows XP Home Edition, Windows Server 2003, Internet Explorer 7.0, Windows Vista, Windows Server 2008, Internet Explorer 8, Windows 7	Yes
Feb-11	**MS11- 004**	Vulnerability in Internet Information Services (IIS) FTP Service Could Allow Remote Code Execution (2489256)	IIS FTP Service Heap Buffer Overrun Vulnerability (CVE-2010-2972)	Important	Remote Code Execution	Windows Vista, Internet Information Services 7.0, Windows Server 2008, Windows 7	No
Feb-11	**MS11- 007**	Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376)	OpenType Font Encoded Character Vulnerability (CVE-2011-033)	Critical	Remote Code Execution	Windows Server 2003, Windows XP, Windows 7, Windows Server 2008, Windows Vista	No
Feb-11	**MS11- 009**	Vulnerability in JScript and VBScript Scripting Engines Could Allow Information Disclosure (2475792)	Scripting Engines Information Disclosure Vulnerability (CVE-2011-0031)	Important	Information Disclosure	Windows 7, Windows Server 2008	No

Feb-11	**MS11-011**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802)	Driver Improper Interaction with Windows Kernel Vulnerability (CVE-2010-4398)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Feb-11	**MS11-011**	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802)	Windows Kernel Integer Truncation Vulnerability (CVE-2011-0045)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows 7	No
Feb-11	**MS11-012**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628)	Win32k Improper User Input Validation Vulnerability (CVE-2011-0086)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows 7, Windows Server 2008, Windows Vista	No
Feb-11	**MS11-012**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628)	Win32k Insufficient User Input Validation Vulnerability (CVE-2011-0087)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows 7, Windows Server 2008, Windows Vista	No
Feb-11	**MS11-012**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628)	Win32k Window Class Pointer Confusion Vulnerability (CVE-2011-0088)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows 7, Windows Server 2008, Windows Vista	No
Feb-11	**MS11-012**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628)	Win32k Window Class Improper Pointer Validation Vulnerability (CVE-2011-0089)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows 7, Windows Server 2008, Windows Vista	No
Feb-11	**MS11-012**	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628)	Win32k Memory Corruption Vulnerability (CVE-2011-0090)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows 7, Windows Server 2008, Windows Vista	No

Feb-11	**MS11- 013**	Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930)	Kerberos Unkeyed Checksum Vulnerability (CVE-2011-0043)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows 7, Windows Server 2008	No
Feb-11	**MS11- 013**	Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930)	Kerberos Spoofing Vulnerability (CVE-2011-0091)	Important	Elevation of Privilege	Windows Server 2003, Windows XP, Windows 7, Windows Server 2008	No
Mar-11	**MS11- 05**	Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030)	DirectShow Insecure Library Loading Vulnerability (CVE-2011-0032)	Critical	Remote Code Execution	Windows XP, Windows 7, Windows Server 2008, Windows Vista, Windows Vista, Windows XP Media Center Edition 2005	Yes
Mar-11	**MS11- 05**	Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030)	DVR-MS Vulnerability (CVE-2011-0042)	Critical	Remote Code Execution	Windows XP, Windows 7, Windows Server 2008, Windows Vista, Windows Vista, Windows XP Media Center Edition 2005	Yes
Mar-11	**MS11- 017**	Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2508062)	Remote Desktop Insecure Library Loading Vulnerability (CVE-2011-0029)	Important	Remote Code Execution	Windows Server 2003, Windows XP, Windows Server 2008, Windows Vista, Windows Vista, Windows 7	No

Contact Information

For more information about this report or if you have any questions, please contact:

BeyondTrust - Corporate Headquarters
30401 Agoura Rd., Suite 200
Agoura Hills, CA 91301
+1 800-234-9072 (tel)
info@beyondtrust.com

