

# BeyondTrust 2009 Microsoft Vulnerability Analysis

**90% of Critical Microsoft Windows 7 Vulnerabilities are Mitigated by Eliminating Admin Rights**

## **Abstract**

This BeyondTrust report investigates all vulnerabilities published in Microsoft's 2009 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, including Windows 7 and Internet Explorer 8. The results show that despite unpredictable and evolving attacks companies can greatly reduce risk, experience greater protection from zero-day threats and reduce the threat from vulnerabilities by removing administrator rights.



[www.beyondtrust.com](http://www.beyondtrust.com)

BeyondTrust – Corporate Headquarters  
30401 Agoura Road, Suite 200  
Agoura Hills, CA 91301 USA  
Phone: +1 800-234-9072

## Table of Contents

<b>Executive Summary</b> .....	3
<b>Section 1: Analysis of All 2009 Microsoft Vulnerabilities</b> .....	4
<b>Section 2: Analysis of All Windows 7 Vulnerabilities to Date</b> .....	7
<b>Conclusion</b> .....	8
<b>About BeyondTrust</b> .....	9
<b>About BeyondTrust Privilege Manager</b> .....	9
<b>Appendix</b> .....	10
<b>Contact Information</b> .....	37

## Executive Summary

Microsoft and their partners regularly identify new security vulnerabilities in Microsoft software. In 2009 Microsoft published nearly 75 security bulletins documenting and providing patches for nearly 200 vulnerabilities. By examining all of the published Microsoft vulnerabilities in 2009 and all of the published Windows 7 vulnerabilities to date, this report quantifies 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:

- 90% of Critical Windows 7 vulnerabilities reported to date
- 100% of Microsoft Office vulnerabilities reported in 2009
- 94% of Internet Explorer and 100% of IE 8 vulnerabilities reported in 2009
- 64% of all Microsoft vulnerabilities reported in 2009

Microsoft is to be lauded for releasing patches to known vulnerabilities each month. However, vulnerabilities take time to identify and patches take time to apply. During this period, threats can damage a corporate network and gain access to sensitive information. It is important that companies follow general best practices to improve security. As companies migrate to 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 the Data Collection and Analysis

Microsoft publishes a Security Bulletin Summary each month to notify customers of the security updates they have made to address vulnerabilities in Microsoft products. The security updates are released on the second Tuesday of the month, 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 2009 and Q1 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 2009. 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, Affected Software, as well as to determine if removing administrator rights will mitigate a vulnerability. 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 2009 Microsoft Vulnerabilities

**100% of Microsoft Office vulnerabilities are mitigated by configuring users to operate without administrator rights.**

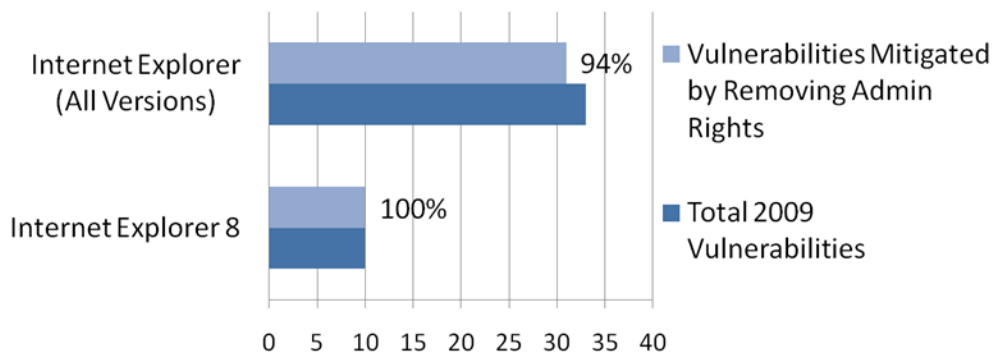
Microsoft Office provides some of the most widely used software applications in the world. Given the prevalence of the software and number of vulnerabilities, increased security protection is key. In total 55 Microsoft Office vulnerabilities appeared in 2009 Security Bulletins. Of these, all 55 are mitigated by removing administrator rights.



**Figure 1.** All reported 2009 Microsoft Office vulnerabilities are mitigated by removing administrator rights.

**By removing administrator rights companies will be better protected against exploitation of 94% of vulnerabilities in all versions of Internet Explorer, and 100% of those in IE 8.**

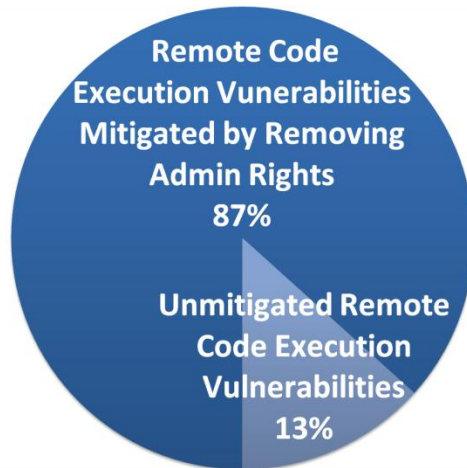
Microsoft released Internet Explorer 8 in March of 2009. It is regarded as the most secure version of the browser. In 2009, there were 33 reported Internet Explorer vulnerabilities. Nearly one third of these vulnerabilities were applicable to Internet Explorer 8. 100% of the Internet Explorer 8 vulnerabilities can be mitigated by removing administrator rights.



**Figure 2.** Reduce the IT security risks associated with Internet Explorer and Internet Explorer 8 vulnerabilities.

**87% of vulnerabilities categorized as Remote Code Execution vulnerabilities are mitigated by removing administrator rights.**

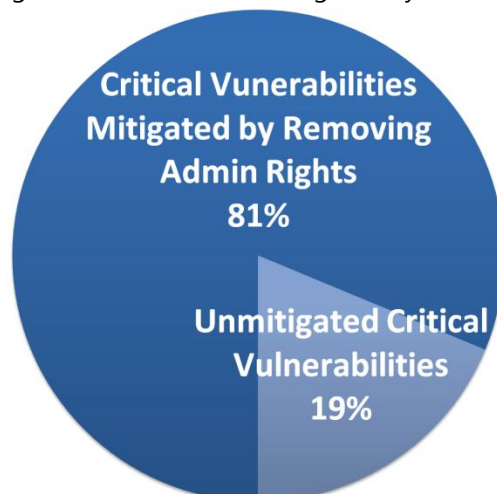
A Vulnerability Impact rating is assigned to each Microsoft Security Bulletin and indicates the effect an exploit of the vulnerabilities may have. Remote Code Execution vulnerabilities may allow someone not at the computer to run unauthorized software and install programs; view, change, or delete data; or create new user accounts. In 2009, there were 135 Remote Code Execution Microsoft vulnerabilities published.



**Figure 3.** The risks associated with Remote Code Execution vulnerabilities can be greatly diminished by removing administrator rights.

**Companies are better protected against 81% of Critical Microsoft vulnerabilities by configuring users without administrator rights.**

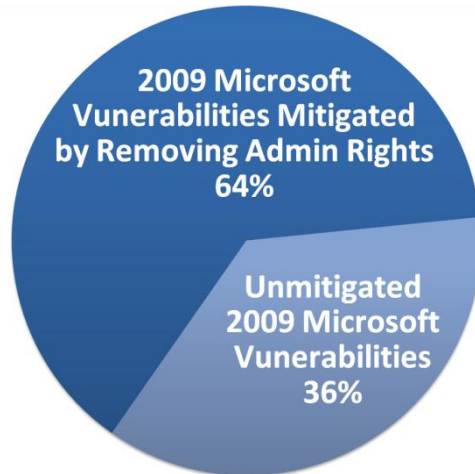
Each Microsoft Security Bulletin is given a severity rating. Critical is the highest rating and indicates that the vulnerabilities are of the highest security concern. In total 80 vulnerabilities appeared in 2009 Security Bulletins with a Critical rating and 65 of these are mitigated by removing administrator rights.



**Figure 4.** Greater than 4 out of 5 of Critical Microsoft vulnerabilities in 2009 are mitigated by removing administrator rights.

**Of the total published Microsoft vulnerabilities, 64% are mitigated by removing administrator rights.**

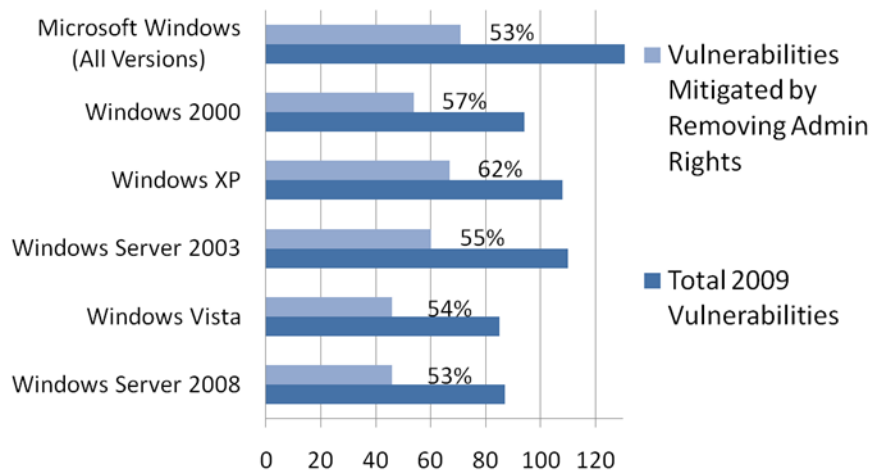
In 2009 there were 190 vulnerabilities published by Microsoft in Security Bulletins. Companies would be better protected against exploitation of 121 of these vulnerabilities by configuring users to run without administrator rights.



**Figure 4.** The vast majority of all 2009 Microsoft vulnerabilities are mitigated by removing admin rights.

**In 2009, exploits of 53% of Windows operating system vulnerabilities can be diminished by configuring users as standard users.**

In 2009 there were 133 published vulnerabilities for all versions of Microsoft operating systems. Companies would be better protected against exploitation of 71 of these vulnerabilities by configuring users to run without administrator rights.

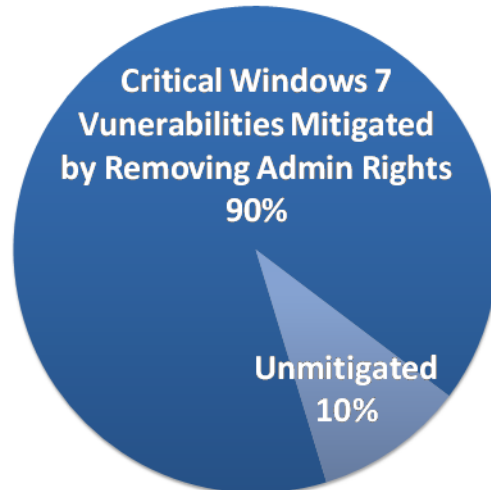


**Figure 5.** Vulnerabilities in Windows operating systems are mitigated by configuring users without administrator rights.

## Section 2: Analysis of All Windows 7 Vulnerabilities to Date

**90% of Critical Windows 7 operating system vulnerabilities are mitigated by having users log in as standard users.**

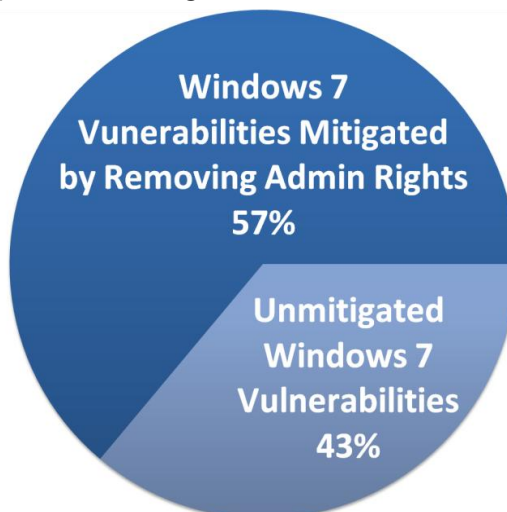
Since the October 2009 release of Windows 7 there have been 10 Critical Windows 7 operating system vulnerabilities published. Companies would be better protected against exploitation of 9 of the Critical Windows 7 vulnerabilities by configuring users without administrator rights.



**Figure 6.** Removing administrator rights is a high priority for Windows 7 rollouts.

**Of all Windows 7 vulnerabilities ever published, 57% are mitigated by removing administrator rights.**

There have been a total of 23 Windows 7 vulnerabilities published to date. The first vulnerability was published in October 2009, the month Windows 7 was publically released. This report captures all Windows 7 vulnerabilities published through March 2010.



**Figure 7.** More than half of all Windows 7 vulnerabilities ever published can be mitigated.

## 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 due to complex corporate environments deploying 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.

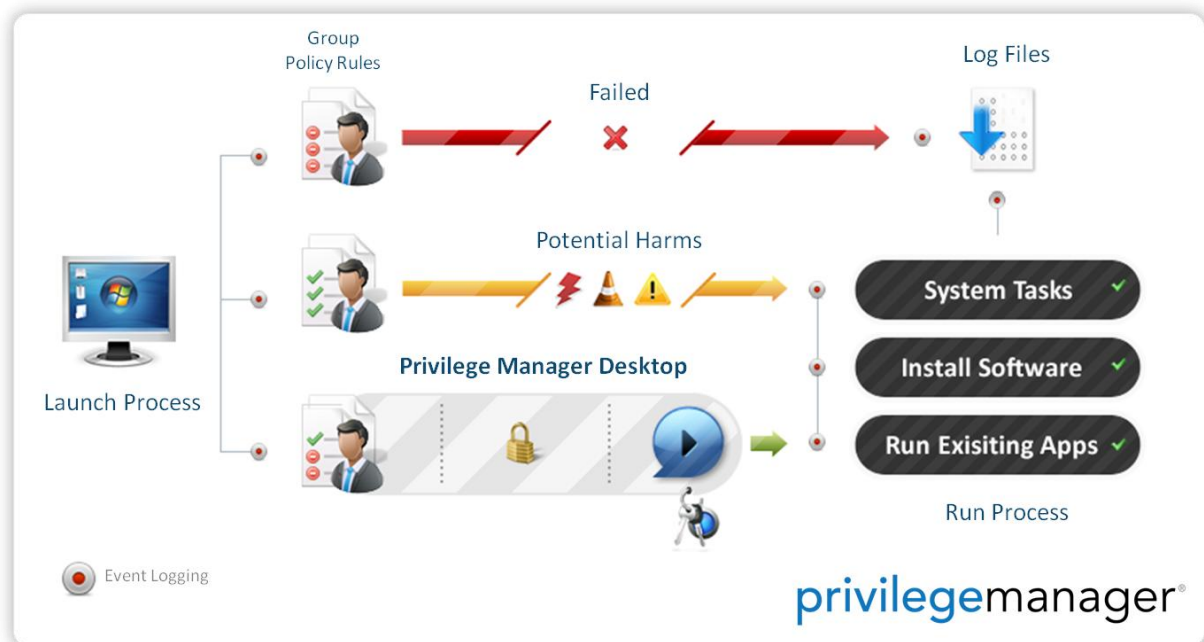
## About BeyondTrust

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 Privileged Access Lifecycle Management (PALM) solutions for 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 Los Angeles, California, with East Coast offices in Greater Boston as well as Washington DC, and EMEA offices in London, UK. For more information, visit [www.beyondtrust.com](http://www.beyondtrust.com).

## About BeyondTrust Privilege Manager

BeyondTrust Privilege Manager, initially released in 2004, is the first Least Privilege Management solution for Windows. Privilege Manager allows end-users to run all required applications, processes and ActiveX controls without administrative privileges. Privilege Manager 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. Privilege Manager 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.

### How Privilege Manager Works:



## Appendix

**Table 1.** All vulnerabilities published in 2009 Microsoft Security Bulletins

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Jan-09	<a href="#">MS09-001</a>	Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	SMB Buffer Overflow Remote Code Execution Vulnerability - CVE-2008-4834	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003	No
Jan-09	<a href="#">MS09-001</a>	Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	SMB Validation Remote Code Execution Vulnerability - CVE-2008-4835	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Jan-09	<a href="#">MS09-001</a>	Vulnerabilities in SMB Could Allow Remote Code Execution (958687)	SMB Validation Denial of Service Vulnerability - CVE-2008-4114	Moderate	Denial of Service	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Feb-09	<a href="#">MS09-002</a>	Cumulative Security Update for Internet Explorer (961260)	Uninitialized Memory Corruption Vulnerability - CVE-2009-0075	Critical	Remote Code Execution	Internet Explorer, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Feb-09	<a href="#">MS09-002</a>	Cumulative Security Update for Internet Explorer (961260)	CSS Memory Corruption Vulnerability - CVE-2009-0076	Critical	Remote Code Execution	Internet Explorer, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Feb-09	<a href="#">MS09-003</a>	Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution (959239)	Memory Corruption Vulnerability - CVE-2009-0098	Critical	Remote Code Execution	Microsoft Exchange Server	No
Feb-09	<a href="#">MS09-003</a>	Vulnerabilities in Microsoft Exchange Could Allow Remote Code Execution (959239)	Literal Processing Vulnerability - CVE-2009-0099	Important	Denial of Service	Microsoft Exchange Server	No
Feb-09	<a href="#">MS09-004</a>	Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420)	SQL Server sp_replwritetovarbin Limited Memory Overwrite Vulnerability - CVE-2008-5416	Important	Remote Code Execution	Microsoft SQL Server	No

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Feb-09	<a href="#">MS09-005</a>	Vulnerabilities in Microsoft Office Visio Could Allow Remote Code Execution (957634)	Memory Validation Vulnerability - CVE-2009-0095	Important	Remote Code Execution	Microsoft Office	Yes
Feb-09	<a href="#">MS09-005</a>	Vulnerabilities in Microsoft Office Visio Could Allow Remote Code Execution (957634)	Memory Corruption Vulnerability - CVE-2009-0096	Important	Remote Code Execution	Microsoft Office	Yes
Feb-09	<a href="#">MS09-005</a>	Vulnerabilities in Microsoft Office Visio Could Allow Remote Code Execution (957634)	Memory Corruption Vulnerability - CVE-2009-0097	Important	Remote Code Execution	Microsoft Office	Yes
Mar-09	<a href="#">MS09-006</a>	Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)	Windows Kernel Input Validation Vulnerability - CVE-2009-0081	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Mar-09	<a href="#">MS09-006</a>	Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)	Windows Kernel Handle Validation Vulnerability - CVE-2009-0082	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Mar-09	<a href="#">MS09-006</a>	Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)	Windows Kernel Invalid Pointer Vulnerability - CVE-2009-0083	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003	No
Mar-09	<a href="#">MS09-007</a>	Vulnerability in SChannel Could Allow Spoofing (960225)	SChannel Spoofing Vulnerability - CVE-2009-0085	Important	Spoofing	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Mar-09	<a href="#">MS09-008</a>	Vulnerabilities in DNS and WINS Server Could Allow Spoofing (962238)	DNS Server Query Validation Vulnerability - CVE-2009-0233	Important	Spoofing	Windows 2000, Windows Server 2003, Windows Server 2008	No
Mar-09	<a href="#">MS09-008</a>	Vulnerabilities in DNS and WINS Server Could Allow Spoofing (962238)	DNS Server Response Validation Vulnerability - CVE-2009-0234	Important	Spoofing	Windows 2000, Windows Server 2003, Windows Server 2008	No
Mar-09	<a href="#">MS09-008</a>	Vulnerabilities in DNS and WINS Server Could Allow Spoofing (962238)	DNS Server Vulnerability in WPAD Registration Vulnerability- CVE-2009-0093	Important	Spoofing	Windows 2000, Windows Server 2003	No

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Mar-09	<a href="#">MS09-008</a>	Vulnerabilities in DNS and WINS Server Could Allow Spoofing (962238)	WPAD WINS Server Registration Vulnerability - CVE-2009-0094	Important	Spoofing	Windows 2000, Windows Server 2003	No
Apr-09	<a href="#">MS09-010</a>	Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (960477)	WordPad and Office Text Converter Memory Corruption Vulnerability - CVE-2009-0087	Important	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Microsoft Office	Yes
Apr-09	<a href="#">MS09-010</a>	Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (960477)	WordPad Word 97 Text Converter Stack Overflow Vulnerability - CVE-2008-4841	Important	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003	Yes
Apr-09	<a href="#">MS09-010</a>	Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (960477)	Word 2000 WordPerfect 6.x Converter Stack Corruption Vulnerability - CVE-2009-0088	Important	Remote Code Execution	Microsoft Office	Yes
Apr-09	<a href="#">MS09-010</a>	Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (960477)	WordPad Word 97 Text Converter Stack Overflow Vulnerability - CVE-2009-0235	Important	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003	Yes
Apr-09	<a href="#">MS09-013</a>	Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)	Windows HTTP Services Integer Underflow Vulnerability - CVE-2009-0086	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Apr-09	<a href="#">MS09-013</a>	Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)	Windows HTTP Services Certificate Name Mismatch Vulnerability - CVE-2009-0089	Important	Spoofing	Windows 2000, Windows XP, Windows Server 2003, Windows Vista	No
Apr-09	<a href="#">MS09-013</a>	Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)	Windows HTTP Services Credential Reflection Vulnerability - CVE-2009-0550	Important	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Apr-09	<a href="#">MS09-011</a>	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (961373)	MJPEG Decompression Vulnerability - CVE-2009-0084	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003	Yes
Apr-09	<a href="#">MS09-014</a>	Cumulative Security Update for Internet Explorer (963027)	Blended Threat Remote Code Execution Vulnerability - CVE-	Moderate	Remote Code Execution	Internet Explorer, Windows XP	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
			2008-2540				
Apr-09	<a href="#">MS09-014</a>	Cumulative Security Update for Internet Explorer (963027)	Blended Threat Remote Code Execution Vulnerability - CVE-2008-2540	Important	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Apr-09	<a href="#">MS09-014</a>	Cumulative Security Update for Internet Explorer (963027)	Page Transition Memory Corruption Vulnerability - CVE-2009-0551	Critical	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Apr-09	<a href="#">MS09-014</a>	Cumulative Security Update for Internet Explorer (963027)	Uninitialized Memory Corruption Vulnerability - CVE-2009-0552	Critical	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Windows Server 2003	Yes
Apr-09	<a href="#">MS09-014</a>	Cumulative Security Update for Internet Explorer (963027)	Uninitialized Memory Corruption Vulnerability - CVE-2009-0553	Critical	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Apr-09	<a href="#">MS09-014</a>	Cumulative Security Update for Internet Explorer (963027)	Uninitialized Memory Corruption Vulnerability - CVE-2009-0554	Critical	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Apr-09	<a href="#">MS09-009</a>	Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution (968557)	Memory Corruption Vulnerability - CVE-2009-0100	Important	Remote Code Execution	Microsoft Office	Yes
Apr-09	<a href="#">MS09-009</a>	Vulnerabilities in Microsoft Office Excel Could Cause Remote Code Execution	Memory Corruption Vulnerability - CVE-2009-0238	Important	Remote Code Execution	Microsoft Office	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
		(968557)					
Apr-09	<a href="#">MS09-012</a>	Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)	Windows MSDTC Service Isolation Vulnerability - CVE-2008-1436	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Apr-09	<a href="#">MS09-012</a>	Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)	Windows WMI Service Isolation Vulnerability - CVE-2009-0078	Important	Elevation of Privilege	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Apr-09	<a href="#">MS09-012</a>	Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)	Windows RPCSS Service Isolation Vulnerability - CVE-2009-0079	Important	Elevation of Privilege	Windows XP, Windows Server 2003	No
Apr-09	<a href="#">MS09-012</a>	Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)	Windows Thread Pool ACL Weakness Vulnerability - CVE-2009-0080	Important	Elevation of Privilege	Windows Vista, Windows Server 2008	No
Apr-09	<a href="#">MS09-016</a>	Vulnerabilities in Microsoft ISA Server and Forefront Threat Management Gateway (Medium Business Edition) Could Cause Denial of Service (961759)	Web Proxy TCP State Limited Denial of Service Vulnerability - CVE-2009-0077	Important	Denial of Service	Microsoft Forefront, Microsoft Internet Security Acceleration Server	No
Apr-09	<a href="#">MS09-016</a>	Vulnerabilities in Microsoft ISA Server and Forefront Threat Management Gateway (Medium Business Edition) Could Cause Denial of Service (961759)	Cross-Site Scripting Vulnerability - CVE-2009-0237	Moderate	Spoofing, Information Disclosure	Microsoft Forefront, Microsoft Internet Security Acceleration Server	No
Apr-09	<a href="#">MS09-015</a>	Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426)	Blended Threat Elevation of Privilege Vulnerability - CVE-2008-2540	Moderate	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	Legacy File Format Vulnerability - CVE-2009-0220	Critical	Remote Code Execution	Microsoft Office	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	Integer Overflow Vulnerability - CVE-2009-0221	Important	Remote Code Execution	Microsoft Office	Yes
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	Legacy File Format Vulnerability - CVE-2009-0222	Critical	Remote Code Execution	Microsoft Office	Yes
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	Legacy File Format Vulnerability - CVE-2009-0223	Critical	Remote Code Execution	Microsoft Office	Yes
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	Memory Corruption Vulnerability - CVE-2009-0224	Important	Remote Code Execution	Microsoft Office	Yes
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	PP7 Memory Corruption Vulnerability - CVE-2009-0225	Important	Remote Code Execution	Microsoft Office	Yes
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	Legacy File Format Vulnerability - CVE-2009-0226	Important	Remote Code Execution	Microsoft Office	Yes
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	Legacy File Format Vulnerability - CVE-2009-0227	Important	Remote Code Execution	Microsoft Office	Yes
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	Memory Corruption Vulnerability - CVE-2009-0556	Important	Remote Code Execution	Microsoft Office	Yes
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	PP7 Memory Corruption Vulnerability - CVE-2009-1128	Important	Remote Code Execution	Microsoft Office	Yes
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	PP7 Memory Corruption Vulnerability - CVE-2009-1129	Important	Remote Code Execution	Microsoft Office	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	Heap Corruption Vulnerability - CVE-2009-1130	Important	Remote Code Execution	Microsoft Office	Yes
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	Data Out of Bounds Vulnerability - CVE-2009-1131	Important	Remote Code Execution	Microsoft Office	Yes
May-09	<a href="#">MS09-017</a>	Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (967340)	Legacy File Format Vulnerability - CVE-2009-1137	Important	Remote Code Execution	Microsoft Office	Yes
Jun-09	<a href="#">MS09-018</a>	Vulnerabilities in Active Directory Could Allow Remote Code Execution (971055)	Active Directory Invalid Free Vulnerability - CVE-2009-1138	Critical	Remote Code Execution	Active Directory Application Mode (ADAM), Windows 2000	No
Jun-09	<a href="#">MS09-018</a>	Vulnerabilities in Active Directory Could Allow Remote Code Execution (971055)	Active Directory Memory Leak Vulnerability - CVE-2009-1139	Important	Denial of Service	Active Directory Application Mode (ADAM), Windows 2000, Windows XP, Windows Server 2003	No
Jun-09	<a href="#">MS09-022</a>	Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Buffer Overflow in Print Spooler Vulnerability - CVE-2009-0228	Critical	Remote Code Execution	Windows 2000	Yes
Jun-09	<a href="#">MS09-022</a>	Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Print Spooler Read File Vulnerability - CVE-2009-0229	Moderate	Information Disclosure	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Jun-09	<a href="#">MS09-022</a>	Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)	Print Spooler Load Library Vulnerability - CVE-2009-0230	Moderate	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Jun-09	<a href="#">MS09-019</a>	Cumulative Security Update for Internet Explorer (969897)	Race Condition Cross-Domain Information Disclosure Vulnerability - CVE-2007-3091	Important	Information Disclosure	Internet Explorer, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Jun-09	<a href="#">MS09-019</a>	Cumulative Security Update for Internet Explorer (969897)	Cross-Domain Information Disclosure Vulnerability - CVE-2009-1140	Important	Information Disclosure	Internet Explorer, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Jun-09	<a href="#">MS09-019</a>	Cumulative Security Update for Internet Explorer (969897)	DHTML Object Memory Corruption Vulnerability - CVE-2009-1141	Moderate	Remote Code Execution	Internet Explorer, Windows XP, Windows Server 2003	Yes
Jun-09	<a href="#">MS09-019</a>	Cumulative Security Update for Internet Explorer (969897)	HTML Object Memory Corruption Vulnerability - CVE-2009-1528	Critical	Remote Code Execution	Internet Explorer, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Jun-09	<a href="#">MS09-019</a>	Cumulative Security Update for Internet Explorer (969897)	Uninitialized Memory Corruption Vulnerability - CVE-2009-1529	Critical	Remote Code Execution	Internet Explorer, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Jun-09	<a href="#">MS09-019</a>	Cumulative Security Update for Internet Explorer (969897)	HTML Objects Memory Corruption Vulnerability - CVE-2009-1530	Critical	Remote Code Execution	Internet Explorer, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Jun-09	<a href="#">MS09-019</a>	Cumulative Security Update for Internet Explorer (969897)	HTML Object Memory Corruption Vulnerability - CVE-2009-1531	Critical	Remote Code Execution	Internet Explorer, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Jun-09	<a href="#">MS09-019</a>	Cumulative Security Update for Internet Explorer (969897)	HTML Objects Memory Corruption Vulnerability - CVE-2009-1532	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Jun-09	<a href="#">MS09-027</a>	Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (969514)	Word Buffer Overflow Vulnerability - CVE-2009-0563	Important	Remote Code Execution	Microsoft Office	Yes
Jun-09	<a href="#">MS09-027</a>	Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (969514)	Word Buffer Overflow Vulnerability - CVE-2009-0565	Important	Remote Code Execution	Microsoft Office	Yes
Jun-09	<a href="#">MS09-021</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)	Record Pointer Corruption Vulnerability - CVE-2009-0549	Important	Remote Code Execution	Microsoft Office	Yes
Jun-09	<a href="#">MS09-021</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)	Object Record Corruption Vulnerability - CVE-2009-0557	Important	Remote Code Execution	Microsoft Office	Yes
Jun-09	<a href="#">MS09-021</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)	Array Indexing Memory Corruption Vulnerability - CVE-2009-0558	Important	Remote Code Execution	Microsoft Office	Yes
Jun-09	<a href="#">MS09-021</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)	String Copy Stack-Based Overrun Vulnerability - CVE-2009-0559	Important	Remote Code Execution	Microsoft Office	Yes
Jun-09	<a href="#">MS09-021</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)	Field Sanitization Memory Corruption Vulnerability - CVE-2009-0560	Important	Remote Code Execution	Microsoft Office	Yes
Jun-09	<a href="#">MS09-021</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)	Record Integer Overflow Vulnerability - CVE-2009-0561	Important	Remote Code Execution	Microsoft Office	Yes
Jun-09	<a href="#">MS09-021</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (969462)	Record Pointer Corruption Vulnerability - CVE-2009-1134	Important	Remote Code Execution	Microsoft Office	Yes
Jun-09	<a href="#">MS09-024</a>	Vulnerability in Microsoft Works Converters Could Allow Remote Code Execution (957632)	File Converter Buffer Overflow Vulnerability - CVE-2009-1533	Important	Remote Code Execution	Microsoft Office	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Jun-09	<a href="#">MS09-026</a>	Vulnerability in RPC Could Allow Elevation of Privilege (970238)	RPC Marshalling Engine Vulnerability - CVE-2009-0568	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Jun-09	<a href="#">MS09-025</a>	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)	Windows Kernel Desktop Vulnerability- CVE-2009-1123	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Jun-09	<a href="#">MS09-025</a>	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)	Windows Kernel Pointer Validation Vulnerability- CVE-2009-1124	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Jun-09	<a href="#">MS09-025</a>	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)	Windows Driver Class Registration Vulnerability - CVE-2009-1125	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Jun-09	<a href="#">MS09-025</a>	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)	Windows Desktop Parameter Edit Vulnerability - CVE-2009-1126	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003	No
Jun-09	<a href="#">MS09-020</a>	Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)	IIS 5.0 WebDAV Authentication Bypass Vulnerability - CVE-2009-1122	Important	Elevation of Privilege	Microsoft Internet Information Services (IIS), Windows 2000	No
Jun-09	<a href="#">MS09-020</a>	Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)	IIS 5.1 and 6.0 WebDAV Authentication Bypass Vulnerability - CVE-2009-1535	Important	Elevation of Privilege	Microsoft Internet Information Services (IIS), Windows XP, Windows Server 2003	No
Jun-09	<a href="#">MS09-023</a>	Vulnerability in Windows Search Could Allow Information Disclosure (963093)	Script Execution in Windows Search Vulnerability - CVE-2009-0239	Moderate	Information Disclosure	Window Search, Windows XP, Windows Server 2003	No
Jul-09	<a href="#">MS09-029</a>	Vulnerabilities in the Embedded OpenType Font Engine Could Allow Remote Code	Embedded OpenType Font Heap Overflow Vulnerability - CVE-	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
		Execution (961371)	2009-0231			Vista, Windows Server 2008	
Jul-09	<a href="#">MS09-029</a>	Vulnerabilities in the Embedded OpenType Font Engine Could Allow Remote Code Execution (961371)	Embedded OpenType Font Integer Overflow Vulnerability - CVE-2009-0232	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Jul-09	<a href="#">MS09-028</a>	Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (971633)	DirectX NULL Byte Overwrite Vulnerability - CVE-2009-1537	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003	Yes
Jul-09	<a href="#">MS09-028</a>	Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (971633)	DirectX Pointer Validation Vulnerability - CVE-2009-1538	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003	Yes
Jul-09	<a href="#">MS09-028</a>	Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (971633)	DirectX Size Validation Vulnerability - CVE-2009-1539	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003	Yes
Jul-09	<a href="#">MS09-032</a>	Cumulative Security Update of ActiveX Kill Bits (973346)	Microsoft Video ActiveX Control Vulnerability - CVE-2008-0015	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003	Yes
Jul-09	<a href="#">MS09-034</a>	Cumulative Security Update for Internet Explorer (972260)	Memory Corruption Vulnerability - CVE-2009-1917	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Jul-09	<a href="#">MS09-034</a>	Cumulative Security Update for Internet Explorer (972260)	HTML Objects Memory Corruption Vulnerability - CVE-2009-1918	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Jul-09	<a href="#">MS09-034</a>	Cumulative Security Update for Internet Explorer (972260)	Uninitialized Memory Corruption Vulnerability - CVE-2009-1919	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Jul-09	<a href="#">MS09-033</a>	Vulnerability in Virtual PC and Virtual Server Could Allow Elevation of Privilege (969856)	Virtual PC and Virtual Server Privileged Instruction Decoding Vulnerability - CVE-2009-1542	Important	Elevation of Privilege	Microsoft Virtual PC, Microsoft Virtual Server	No
Jul-09	<a href="#">MS09-031</a>	Vulnerability in Virtual PC and Virtual Server Could Allow Elevation of Privilege (969856)	Radius OTP Bypass Vulnerability - CVE-2009-1135	Important	Elevation of Privilege	Microsoft Internet Security Acceleration Server 2006	No
Jul-09	<a href="#">MS09-030</a>	Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (969516)	Pointer Dereference Vulnerability - CVE-2009-0566	Important	Remote Code Execution	Microsoft Office	Yes
Jul-09	<a href="#">MS09-035</a>	Vulnerabilities in Visual Studio Active Template Library Could Allow Remote Code Execution (969706)	ATL Uninitialized Object Vulnerability - CVE-2009-0901	Moderate	Remote Code Execution	Microsoft Visual Studio, Windows Embedded CE	Yes
Jul-09	<a href="#">MS09-035</a>	Vulnerabilities in Visual Studio Active Template Library Could Allow Remote Code Execution (969706)	ATL COM Initialization Vulnerability - CVE-2009-2493	Moderate	Remote Code Execution	Microsoft Visual Studio, Windows Embedded CE	Yes
Jul-09	<a href="#">MS09-035</a>	Vulnerabilities in Visual Studio Active Template Library Could Allow Remote Code Execution (969706)	ATL Null String Vulnerability - CVE-2009-2495	Moderate	Information Disclosure	Microsoft Visual Studio, Windows Embedded CE	Yes
Aug-09	<a href="#">MS09-043</a>	Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (957638)	Office Web Components Memory Allocation Vulnerability - CVE-2009-0562	Critical	Remote Code Execution	Microsoft Office, Microsoft Internet Security and Acceleration Server	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Aug-09	<a href="#">MS09-043</a>	Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (957638)	Office Web Components Heap Corruption Vulnerability - CVE-2009-2496	Critical	Remote Code Execution	Microsoft Office, Microsoft Internet Security and Acceleration Server	Yes
Aug-09	<a href="#">MS09-043</a>	Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (957638)	Office Web Components HTML Script Vulnerability - CVE-2009-1136	Critical	Remote Code Execution	Microsoft Office, Microsoft Internet Security and Acceleration Server	Yes
Aug-09	<a href="#">MS09-043</a>	Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution (957638)	Office Web Components Buffer Overflow Vulnerability - CVE-2009-1534	Critical	Remote Code Execution	Microsoft Office, Microsoft Visual Studio	Yes
Aug-09	<a href="#">MS09-044</a>	Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (970927)	Remote Desktop Connection Heap Overflow Vulnerability - CVE-2009-1133	Critical	Remote Code Execution	Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Aug-09	<a href="#">MS09-044</a>	Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution (970927)	Remote Desktop Connection ActiveX Control Heap Overflow Vulnerability - CVE-2009-1929	Critical	Remote Code Execution	Windows XP, Windows Vista, Windows Server 2008	Yes
Aug-09	<a href="#">MS09-039</a>	Vulnerabilities in WINS Could Allow Remote Code Execution (969883)	WINS Heap Overflow Vulnerability - CVE-2009-1923	Critical	Remote Code Execution	Windows Server 2000, Windows Server 2003	No
Aug-09	<a href="#">MS09-039</a>	Vulnerabilities in WINS Could Allow Remote Code Execution (969883)	WINS Integer Overflow Vulnerability - CVE-2009-1924	Critical	Remote Code Execution	Windows Server 2000	No
Aug-09	<a href="#">MS09-038</a>	Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (971557)	Malformed AVI Header Vulnerability - CVE-2009-1545	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Aug-09	<a href="#">MS09-038</a>	Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (971557)	AVI Integer Overflow Vulnerability - CVE-2009-1546	Important	Denial of Service	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
						Server 2008	
Aug-09	<a href="#">MS09-037</a>	Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908)	Microsoft Video ActiveX Control Vulnerability - CVE-2008-0015	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Aug-09	<a href="#">MS09-037</a>	Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908)	ATL Header Memcopy Vulnerability - CVE-2008-0020	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Aug-09	<a href="#">MS09-037</a>	Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908)	ATL Uninitialized Object Vulnerability - CVE-2009-0901	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Aug-09	<a href="#">MS09-037</a>	Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908)	ATL COM Initialization Vulnerability - CVE-2009-2493	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Aug-09	<a href="#">MS09-037</a>	Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution (973908)	ATL Object Type Mismatch Vulnerability - CVE-2009-2494	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Aug-09	<a href="#">MS09-041</a>	Vulnerability in Workstation Service Could Allow Elevation of Privilege (971657)	Workstation Service Memory Corruption Vulnerability - CVE-2009-1544	Important	Elevation of Privilege	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Aug-09	<a href="#">MS09-040</a>	Vulnerability in Message Queuing Could Allow Elevation of Privilege (971032)	MSMQ Null Pointer Vulnerability - CVE-2009-1922	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista	No
Aug-09	<a href="#">MS09-036</a>	Vulnerability in ASP.NET in Microsoft Windows Could Allow Denial of Service (970957)	Remote Unauthenticated Denial of Service in ASP.NET Vulnerability - CVE-2009-1536	Important	Denial of Service	Microsoft .NET, Windows Server 2003, Windows Vista	No

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Aug-09	<a href="#">MS09-042</a>	Vulnerability in Telnet Could Allow Remote Code Execution (960859)	Telnet Credential Reflection Vulnerability - CVE-2009-1930	Important	Remote Code Execution	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Sep-09	<a href="#">MS09-045</a>	Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution (971961)	JScript Remote Code Execution Vulnerability - CVE-2009-1920	Critical	Remote Code Execution	Windows 2000, Windows Server 2003, Windows XP, Windows Vista, Windows Server 2008	Yes
Sep-09	<a href="#">MS09-049</a>	Vulnerability in Wireless LAN AutoConfig Service Could Allow Remote Code Execution (970710)	Wireless Frame Parsing Remote Code Execution Vulnerability - CVE-2009-1132	Important	Remote Code Execution	Windows Vista, Windows Server 2008	No
Sep-09	<a href="#">MS09-047</a>	Vulnerabilities in Windows Media Format Could Allow Remote Code Execution (973812)	Windows Media Header Parsing Invalid Free Vulnerability - CVE-2009-2498	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Sep-09	<a href="#">MS09-047</a>	Vulnerabilities in Windows Media Format Could Allow Remote Code Execution (973812)	Windows Media Playback Memory Corruption Vulnerability - CVE-2009-2499	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Sep-09	<a href="#">MS09-048</a>	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723)	TCP/IP Zero Window Size Vulnerability - CVE-2008-4609	Important	Denial of Service	Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Sep-09	<a href="#">MS09-048</a>	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723)	TCP/IP Timestamps Code Execution Vulnerability - CVE-2009-1925	Critical	Remote Code Execution	Windows Vista, Windows Server 2008	No
Sep-09	<a href="#">MS09-048</a>	Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723)	TCP/IP Orphaned Connections Vulnerability - CVE-2009-1926	Important	Denial of Service	Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Sep-09	<a href="#">MS09-046</a>	Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (956844)	DHTML Editing Component ActiveX Control Vulnerability - CVE-2009-2519	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Oct-09	<a href="#">MS09-050</a>	Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)	SMBv2 Infinite Loop Vulnerability - CVE-2009-2526	Important	Denial of Service	Windows Vista, Windows Server 2008	No
Oct-09	<a href="#">MS09-050</a>	Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)	SMBv2 Command Value Vulnerability - CVE-2009-2532	Critical	Remote Code Execution	Windows Vista, Windows Server 2008	No
Oct-09	<a href="#">MS09-050</a>	Vulnerabilities in SMBv2 Could Allow Remote Code Execution (975517)	SMBv2 Negotiation Vulnerability - CVE-2009-3103	Critical	Remote Code Execution	Windows Vista, Windows Server 2008	No
Oct-09	<a href="#">MS09-051</a>	Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution (975682)	Windows Media Runtime Voice Sample Rate Vulnerability - CVE-2009-0555	Critical	Remote Code Execution	Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Oct-09	<a href="#">MS09-051</a>	Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution (975682)	Windows Media Runtime Heap Corruption Vulnerability - CVE-2009-2525	Critical	Remote Code Execution	Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Oct-09	<a href="#">MS09-052</a>	Vulnerability in Windows Media Player Could Allow Remote Code Execution (974112)	WMP Heap Overflow Vulnerability - CVE-2009-2527	Critical	Remote Code Execution	Windows Media, Windows 2000, Windows XP, Windows Server 2003	Yes
Oct-09	<a href="#">MS09-054</a>	Cumulative Security Update for Internet Explorer (974455)	Data Stream Header Corruption Vulnerability - CVE-2009-1547	Critical	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Oct-09	<a href="#">MS09-054</a>	Cumulative Security Update for Internet Explorer (974455)	HTML Component Handling Vulnerability - CVE-2009-2529	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Oct-09	<a href="#">MS09-054</a>	Cumulative Security Update for Internet Explorer (974455)	Uninitialized Memory Corruption Vulnerability - CVE-2009-2530	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Oct-09	<a href="#">MS09-054</a>	Cumulative Security Update for Internet Explorer (974455)	Uninitialized Memory Corruption Vulnerability - CVE-2009-2531	Moderate	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Oct-09	<a href="#">MS09-055</a>	Cumulative Security Update of ActiveX Kill Bits (973525)	ATL COM Initialization Vulnerability- CVE-2009-2493	Moderate	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Oct-09	<a href="#">MS09-060</a>	Vulnerabilities in Microsoft Active Template Library (ATL) ActiveX Controls for Microsoft Office Could Allow Remote Code Execution (973965)	ATL Uninitialized Object Vulnerability - CVE-2009-0901	Critical	Remote Code Execution	Microsoft Outlook, Microsoft Office, Microsoft Visio	Yes
Oct-09	<a href="#">MS09-060</a>	Vulnerabilities in Microsoft Active Template Library (ATL) ActiveX Controls for Microsoft Office Could Allow Remote Code Execution (973965)	ATL COM Initialization Vulnerability - CVE-2009-2493	Critical	Remote Code Execution	Microsoft Outlook, Microsoft Office, Microsoft Visio	Yes
Oct-09	<a href="#">MS09-060</a>	Vulnerabilities in Microsoft Active Template Library (ATL) ActiveX Controls for Microsoft Office Could Allow Remote Code Execution (973965)	ATL Null String Vulnerability - CVE-2009-2495	Moderate	Information Disclosure	Microsoft Outlook, Microsoft Office, Microsoft Visio	Yes
Oct-09	<a href="#">MS09-061</a>	Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow	Microsoft .NET Framework Pointer Verification Vulnerability - CVE-	Critical	Remote Code Execution	Microsoft .NET, Windows 2000, Windows XP, Windows Server	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
		Remote Code Execution (974378)	2009-0090			2003, Windows Vista, Windows Server 2008	
Oct-09	<a href="#">MS09-061</a>	Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution (974378)	Microsoft .NET Framework Type Verification Vulnerability - CVE-2009-0091	Critical	Remote Code Execution	Microsoft .NET, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Oct-09	<a href="#">MS09-061</a>	Vulnerabilities in the Microsoft .NET Common Language Runtime Could Allow Remote Code Execution (974378)	Microsoft Silverlight and Microsoft .NET Framework CLR Vulnerability - CVE-2009-2497	Critical	Remote Code Execution	Microsoft .NET, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes
Oct-09	<a href="#">MS09-062</a>	Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)	GDI+ WMF Integer Overflow Vulnerability - CVE-2009-2500	Critical	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Microsoft Office, SQL Server, Microsoft Visual Studio, Microsoft Report Viewer, Microsoft Forefront	Yes
Oct-09	<a href="#">MS09-062</a>	Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)	GDI+ PNG Heap Overflow Vulnerability - CVE-2009-2501	Critical	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Microsoft Office, SQL Server, Microsoft Visual Studio, Microsoft Forefront	Yes
Oct-09	<a href="#">MS09-062</a>	Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)	GDI+ TIFF Buffer Overflow Vulnerability - CVE-2009-2502	Critical	Remote Code Execution	Internet Explorer, Microsoft Windows 2000, Windows XP, Microsoft Office, SQL Server, Microsoft Visual	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
						Studio, Microsoft Forefront	
Oct-09	<a href="#">MS09-062</a>	Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)	GDI+ TIFF Memory Corruption Vulnerability - CVE-2009-2503	Critical	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Windows Server 2003, Microsoft Office, SQL Server, Microsoft Report Viewer, Microsoft Forefront	Yes
Oct-09	<a href="#">MS09-062</a>	Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)	GDI+ .NET API Vulnerability - CVE-2009-2504	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Microsoft Office, SQL Server, Microsoft Report Viewer, Microsoft Forefront	Yes
Oct-09	<a href="#">MS09-062</a>	Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)	GDI+ PNG Integer Overflow Vulnerability - CVE-2009-3126	Critical	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Microsoft Office, SQL Server, Microsoft Report Viewer, Microsoft Forefront	Yes
Oct-09	<a href="#">MS09-062</a>	Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)	Memory Corruption Vulnerability - CVE-2009-2528	Critical	Remote Code Execution	Microsoft Office	Yes
Oct-09	<a href="#">MS09-062</a>	Vulnerabilities in GDI+ Could Allow Remote Code Execution (957488)	Office BMP Integer Overflow Vulnerability - CVE-2009-2518	Critical	Remote Code Execution	Microsoft Office	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Oct-09	<a href="#">MS09-053</a>	Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution (975254)	IIS FTP Service DoS Vulnerability - CVE-2009-2521	Important	Denial of Service	Microsoft Internet Information Services (IIS), Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Oct-09	<a href="#">MS09-053</a>	Vulnerabilities in FTP Service for Internet Information Services Could Allow Remote Code Execution (975254)	IIS FTP Service RCE and DoS Vulnerability - CVE-2009-3023	Important	Denial of Service	Microsoft Internet Information Services (IIS), Microsoft Windows 2000, Windows XP, Windows Server 2003	No
Oct-09	<a href="#">MS09-056</a>	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	<a href="#">MS09-056</a>	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	<a href="#">MS09-057</a>	Vulnerability in Indexing Service Could Allow Remote Code Execution (969059)	Memory Corruption in Indexing Service Vulnerability - CVE-2009-2507	Important	Remote Code Execution	Microsoft Windows 2000, Windows XP, Windows Server 2003	Yes
Oct-09	<a href="#">MS09-058</a>	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (971486)	Windows Kernel Integer Underflow Vulnerability - CVE-2009-2515	Moderate	Denial of Service	Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Oct-09	<a href="#">MS09-058</a>	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (971486)	Windows Kernel NULL Pointer Dereference Vulnerability - CVE-2009-2516	Important	Elevation of Privilege	Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Oct-09	<a href="#">MS09-058</a>	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (971486)	Windows Kernel Exception Handler Vulnerability - CVE-2009-2517	Moderate	Denial of Service	Windows Server 2003	No
Oct-09	<a href="#">MS09-059</a>	Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (975467)	Local Security Authority Subsystem Service Integer Overflow Vulnerability - CVE-2009-2524	Important	Denial of Service	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	No
Nov-09	<a href="#">MS09-063</a>	Vulnerability in Web Services on Devices API Could Allow Remote Code Execution (973565)	Web Services on Devices API Memory Corruption Vulnerability - CVE-2009-2512	Critical	Remote Code Execution	Windows Vista, Windows Server 2008	No
Nov-09	<a href="#">MS09-064</a>	Vulnerability in License Logging Server Could Allow Remote Code Execution (974783)	License Logging Server Heap Overflow Vulnerability - CVE-2009-2523	Critical	Remote Code Execution	Windows 2000	No
Nov-09	<a href="#">MS09-065</a>	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947)	Win32k NULL Pointer Dereferencing Vulnerability - CVE-2009-1127	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Nov-09	<a href="#">MS09-065</a>	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947)	Win32k Insufficient Data Validation Vulnerability - CVE-2009-2513	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Nov-09	<a href="#">MS09-065</a>	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947)	Win32k EOT Parsing Vulnerability - CVE-2009-2514	Critical	Remote Code Execution	Windows 2000, Windows XP, Windows Server 2003	No

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Nov-09	<a href="#">MS09-066</a>	Vulnerability in Active Directory Could Allow Denial of Service (973309)	LSASS Recursive Stack Overflow Vulnerability - CVE-2009-1928	Important	Denial of Service	Active Directory Application Mode (ADAM), Windows 2000, Windows XP, Windows Server 2003, Windows Server 2008	No
Nov-09	<a href="#">MS09-067</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652)	Excel Cache Memory Corruption Vulnerability - CVE-2009-3127	Important	Remote Code Execution	Microsoft Office	Yes
Nov-09	<a href="#">MS09-067</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652)	Excel SxView Memory Corruption Vulnerability - CVE-2009-3128	Important	Remote Code Execution	Microsoft Office	Yes
Nov-09	<a href="#">MS09-067</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652)	Excel Featherheader Record Memory Corruption Vulnerability - CVE-2009-3129	Important	Remote Code Execution	Microsoft Office	Yes
Nov-09	<a href="#">MS09-067</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652)	Excel Document Parsing Heap Overflow Vulnerability - CVE-2009-3130	Important	Remote Code Execution	Microsoft Office	Yes
Nov-09	<a href="#">MS09-067</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652)	Excel Formula Parsing Memory Corruption Vulnerability - CVE-2009-3131	Important	Remote Code Execution	Microsoft Office	Yes
Nov-09	<a href="#">MS09-067</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652)	Excel Index Parsing Vulnerability - CVE-2009-3132	Important	Remote Code Execution	Microsoft Office	Yes
Nov-09	<a href="#">MS09-067</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652)	Excel Document Parsing Memory Corruption Vulnerability - CVE-2009-3133	Important	Remote Code Execution	Microsoft Office	Yes
Nov-09	<a href="#">MS09-067</a>	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (972652)	Excel Field Sanitization Vulnerability - CVE-2009-3134	Important	Remote Code Execution	Microsoft Office	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Nov-09	<a href="#">MS09-068</a>	Vulnerability in Microsoft Office Word Could Allow Remote Code Execution (976307)	Microsoft Office Word File Information Memory Corruption Vulnerability - CVE-2009-3135	Important	Remote Code Execution	Microsoft Office	Yes
Dec-09	<a href="#">MS09-071</a>	Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	Internet Authentication Service Memory Corruption Vulnerability - CVE-2009-2505	Critical	Remote Code Execution	Windows Vista, Windows Server 2008	No
Dec-09	<a href="#">MS09-071</a>	Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)	MS-CHAP Authentication Bypass Vulnerability - CVE-2009-3677	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	No
Dec-09	<a href="#">MS09-074</a>	Vulnerability in Microsoft Office Project Could Allow Remote Code Execution (967183)	Project Memory Validation Vulnerability - CVE-2009-0102	Important	Remote Code Execution	Microsoft Office	Yes
Dec-09	<a href="#">MS09-072</a>	Cumulative Security Update for Internet Explorer (976325)	ATL COM Initialization Vulnerability - CVE-2009-2493	Critical	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Windows Server 2003	Yes
Dec-09	<a href="#">MS09-072</a>	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	<a href="#">MS09-072</a>	Cumulative Security Update for Internet Explorer (976325)	HTML Object Memory Corruption Vulnerability - CVE-2009-3672	Critical	Remote Code Execution	Internet Explorer, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Dec-09	<a href="#">MS09-072</a>	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	<a href="#">MS09-072</a>	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
Dec-09	<a href="#">MS09-069</a>	Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (974392)	Local Security Authority Subsystem Service Resource Exhaustion Vulnerability - CVE-2009-3675	Important	Denial of Service	Windows 2000, Windows XP, Windows Server 2003	No
Dec-09	<a href="#">MS09-070</a>	Vulnerabilities in Active Directory Federation Services Could Allow Remote Code Execution (971726)	Single Sign On Spoofing in ADFS Vulnerability - CVE-2009-2508	Moderate	Spoofing	Windows Server 2003, Windows Server 2008	No
Dec-09	<a href="#">MS09-070</a>	Vulnerabilities in Active Directory Federation Services Could Allow Remote Code Execution (971726)	Remote Code Execution in ADFS Vulnerability - CVE-2009-2509	Important	Remote Code Execution	Windows Server 2003, Windows Server 2008	No
Dec-09	<a href="#">MS09-073</a>	Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution (975539)	WordPad and Office Text converter Memory Corruption Vulnerability - CVE-2009-2506	Important	Remote Code Execution	Windows 2000, Windows 2003, Windows XP, Microsoft Office, Microsoft Works	Yes

**Table 2.** All Windows 7 vulnerabilities published to date

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Windows 7 Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Oct-09	<a href="#">MS09-056</a>	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	<a href="#">MS09-056</a>	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	<a href="#">MS09-059</a>	Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service (975467)	Local Security Authority Subsystem Service Integer Overflow Vulnerability - CVE-2009-2524	Important	Denial of Service	Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7	No
Dec-09	<a href="#">MS09-072</a>	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	<a href="#">MS09-072</a>	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	<a href="#">MS09-072</a>	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

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Windows 7 Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Jan-10	<a href="#">MS10-001</a>	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	<a href="#">MS10-002</a>	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	<a href="#">MS10-002</a>	Cumulative Security Update for Internet Explorer (978207)	URL Validation Vulnerability - CVE-2010-0027	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	Yes
Jan-10	<a href="#">MS10-002</a>	Cumulative Security Update for Internet Explorer (978207)	Uninitialized Memory Corruption Vulnerability - CVE-2010-0244	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	Yes
Jan-10	<a href="#">MS10-002</a>	Cumulative Security Update for Internet Explorer (978207)	Uninitialized Memory Corruption Vulnerability - CVE-2010-0245	Low	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	Yes

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Windows 7 Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Jan-10	<a href="#">MS10-002</a>	Cumulative Security Update for Internet Explorer (978207)	Uninitialized Memory Corruption Vulnerability - CVE-2010-0246	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	Yes
Jan-10	<a href="#">MS10-002</a>	Cumulative Security Update for Internet Explorer (978207)	HTML Object Memory Corruption Vulnerability - CVE-2010-0248	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	Yes
Jan-10	<a href="#">MS10-002</a>	Cumulative Security Update for Internet Explorer (978207)	HTML Object Memory Corruption Vulnerability - CVE-2010-0249	Critical	Remote Code Execution	Internet Explorer, Internet Explorer 8, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	Yes
Feb-10	<a href="#">MS10-006</a>	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	<a href="#">MS10-008</a>	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	<a href="#">MS10-013</a>	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

Date	Bulletin ID and Link	Security Bulletin Title	Vulnerability Name	Windows 7 Severity Rating	Impact of Vulnerability	Affected Software	Mitigated by Removing Admin Rights
Feb-10	<a href="#">MS10-012</a>	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	<a href="#">MS10-012</a>	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	SMB Memory Corruption Vulnerability - CVE-2010-0021	Important	Denial of Service	Windows Vista, Windows 7, Windows Server 2008	No
Feb-10	<a href="#">MS10-012</a>	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	SMB Null Pointer Vulnerability - CVE-2010-0022	Important	Denial of Service	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Feb-10	<a href="#">MS10-012</a>	Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)	SMB NTLM Authentication Lack of Entropy Vulnerability - CVE-2010-0231	Important	Elevation of Privilege	Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7, Windows Server 2008	No
Feb-10	<a href="#">MS10-015</a>	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	<a href="#">MS10-016</a>	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

## 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](mailto:info@beyondtrust.com)