



---

## Summary of Critical Patches – February 2008

---

---

### Microsoft Security Bulletin – MS08-007

---

#### Vulnerability in WebDAV Mini-Redirector

##### **MS08-007- Vulnerability in WebDAV Mini-Redirector Could Allow Remote Code**

This critical security update resolves a reported vulnerability in the WebDAV Mini-Redirector by modifying the way that the Mini-Redirector handles long pathnames. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

#### **Affected Software**

Windows XP Service Pack 2  
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2  
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2  
Windows Server 2003 x64 Edition and Windows 2003 Server x64 Edition Service Pack 2  
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium based Systems  
Windows Vista  
Windows Vista x64 Edition

#### **Vulnerability**

##### **CVE-2008-0080- Mini-Redirector Heap Overflow Vulnerability**

A remote code execution vulnerability exists in the way that the WebDAV Mini-Redirector handles responses.

#### **Vulnerability Information**

A Mini-Redirector driver implements a number of callback routines that are used by the Redirected Drive Buffering Subsystem (RDBSS) to communicate with the driver. The Mini-Redirector improperly handles malicious WebDAV responses.

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

#### **Comment / Mitigation**

Systems on which WebDAV client service is enabled are primarily at risk.

- **Web Client services could be disabled by default.**

**References:**

<http://www.microsoft.com/technet/security/bulletin/MS08-007.msp>

---

## Microsoft Security Bulletin – MS08-008

---

### Vulnerability in OLE Automation

#### **MS08-008- Vulnerability in OLE Automation Could Allow Remote Code Execution**

This critical security update resolves a privately reported vulnerability. This vulnerability could allow remote code execution if a user viewed a specially crafted Web page. The vulnerability could be exploited through attacks on Object Linking and Embedding (OLE) Automation.

This security update addresses the vulnerability by adding a check on memory requests within OLE Automation.

#### **Affected Software**

Windows 2000 Service Pack 4

Windows XP Service Pack 2

Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2

Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2

Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2

Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems

Windows Vista

Windows Vista x64 Edition

Microsoft Office 2004 for Mac

#### **Vulnerability**

**CVE-2007-0065-** OLE Heap Overrun Vulnerability

#### **Vulnerability Information**

A remote code execution vulnerability exists in Object Linking and Embedding (OLE) Automation that could allow an attacker who successfully exploited this vulnerability to make changes to the system with the permissions of the logged-on user.

Object linking and embedding (OLE) Automation is a Windows protocol that allows an application to share data or control another application. OLE Automation is an industry standard that applications use to expose their OLE objects to development tools, macro languages, and other containers that support OLE Automation.

#### **Comment / Mitigation**

- **Mitigation set 1 applies.**

#### **References:**

<http://www.microsoft.com/technet/security/bulletin/MS08-008.mspx>

---

## Microsoft Security Bulletin – MS08-009

---

### Vulnerability in Microsoft Word

#### **MS08-009- Vulnerability in Microsoft Word Could Allow Remote Code Execution**

This critical security update resolves one privately reported vulnerability in Microsoft Word that could allow remote code execution if a user opens a specially crafted Word file with a malformed value.

This security update addresses the vulnerability by modifying the way that Microsoft Word handles specially crafted Word files.

#### **Affected Software**

Microsoft Office 2000 Service Pack 3  
Microsoft Office XP Service Pack 3  
Microsoft Office 2003 Service Pack 2  
Microsoft Office 2004 for Mac

#### **Vulnerability**

##### **CVE-2008-0109- Word Memory Corruption Vulnerability**

A remote code execution vulnerability exists in the way that Word handles specially crafted Word files.

#### **Vulnerability Information**

The vulnerability is caused by a memory calculation error when parsing a specially crafted Word file. The error may corrupt system memory in such a way that an attacker could execute arbitrary code.

This vulnerability requires that a user open a specially crafted Word file with an affected version of Microsoft Word.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted Word file to the user and by convincing the user to open the file.

In a Web-based attack scenario, an attacker would have to entice a victim to visit a web site hosting a crafted Word document containing the vulnerability. This includes both malicious web sites and legitimate sites that have been compromised.

Systems where Microsoft Word is used are primarily at risk.

#### **Comment / Mitigation**

- The vulnerability cannot be exploited on Microsoft Office 2007 systems.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful, a user must open an attachment that is sent in an e-mail message.

## Microsoft Monthly Patch Summary - Date: 13<sup>th</sup> February 2008

---

- An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. 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.
- Users who have installed and are using the Office Document Open Confirmation Tool for Office 2000 will be prompted with Open, Save, or Cancel before opening a document. The features of the Office Document Open Confirmation Tool are incorporated in Office XP and later editions of Office.

### References:

<http://www.microsoft.com/technet/security/bulletin/MS08-009.mspx>

---

## Microsoft Security Bulletin – MS08-010

---

### Cumulative Security Update for Internet Explorer

#### MS08-010 Security Updates for Internet Explorer

This critical security update resolves three reported vulnerabilities. The most serious of the vulnerabilities could allow remote code execution if a user viewed a specially crafted Web page using Internet Explorer.

The security update addresses these vulnerabilities by modifying the way that Internet Explorer handles HTML and validates data, as well as by setting the kill bit for an ActiveX control .

#### Affected Software

Microsoft Windows 2000 Service Pack 4  
Microsoft Windows 2000 Service Pack 4  
Windows XP Service Pack 2  
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2  
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2  
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2  
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems

#### Vulnerability

**CVE-2008-0076-** HTML Rendering Memory Corruption Vulnerability

#### Vulnerability Information

A remote code execution vulnerability exists in the way Internet Explorer interprets HTML with certain layout combinations. When Internet Explorer handles these it may corrupt system memory in such a way that an attacker could execute arbitrary code.

#### Comment / Mitigation

- **Mitigation set 1 applies.**

#### Vulnerability

**CVE-2008-0077-** Property Memory Corruption Vulnerability

#### Vulnerability Information

A remote code execution vulnerability exists in the way Internet Explorer handles a property method. An attacker could exploit the vulnerability by constructing a specially crafted Web page.

#### Comment / Mitigation

- Mitigation set 1 applies.

### **Vulnerability**

**CVE-2008-0078-** Argument Handling Memory Corruption Vulnerability

#### **Vulnerability Information**

A remote code execution vulnerability exists in the way Internet Explorer handles argument validation in image processing. An attacker could exploit the vulnerability by constructing a specially crafted Web page.

#### **Comment / Mitigation**

- Mitigation set 1 applies.

### **Vulnerability**

**CVE-2007-4790-** ActiveX Object Memory Corruption Vulnerability

#### **Vulnerability Information**

A remote code execution vulnerability exists in a component of Microsoft Fox Pro. An attacker could exploit the vulnerability by constructing a specially crafted Web page.

#### **Comment / Mitigation**

- Mitigation set 1 applies.

#### **References:**

<http://www.microsoft.com/technet/security/bulletin/MS08-010.msp>

---

## Microsoft Security Bulletin – MS08-012

---

### Vulnerability in Microsoft Office Publisher

**MS08-012-** Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution

This critical security update resolves a reported vulnerability in Microsoft Office Publisher which could allow remote code execution if a user opens a specially crafted Publisher file. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

#### Affected Software

Microsoft Office 2000 Service Pack 3  
Microsoft Office XP Service Pack 3  
Microsoft Office 2003 Service Pack 2

#### Vulnerability

**CVE-2008-0102-** Publisher Invalid Memory Reference Vulnerability

A remote code execution vulnerability exists in the way Microsoft Office Publisher fails to adequately clear out memory resources when loading application data from disk to memory. An attacker could exploit the vulnerability by constructing a specially crafted Publisher (.pub) file. When a user views the .pub file, the vulnerability could allow remote code execution.

**CVE-2008-0104-** Publisher Memory Corruption Vulnerability

A remote code execution vulnerability exists in the way Microsoft Office Publisher fails to properly validate memory index values. An attacker could exploit the vulnerability by constructing a specially crafted Publisher (.pub) file. When a user views the .pub file, the vulnerability could allow remote code execution.

#### Vulnerability Information

These vulnerabilities require that a user open a specially crafted Publisher file with an affected edition of Microsoft Office Publisher.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted file to the user and by convincing the user to open the file.

In a Web-based attack scenario, an attacker would have to entice a victim to visit a web site hosting a crafted Office document containing the vulnerability. This includes both malicious web sites and legitimate sites that have been compromised.

#### Comment / Mitigation

- An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. 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.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful a user must open an attachment that is sent in an e-mail message.

## Microsoft Monthly Patch Summary - Date: 13<sup>th</sup> February 2008

---

- Do not open or save Microsoft Office files that you receive from untrusted sources or that you receive unexpectedly from trusted sources. This vulnerability could be exploited when a user opens a specially crafted file.

### References:

<http://www.microsoft.com/technet/security/bulletin/MS08-012.mspx>

---

## Microsoft Security Bulletin – MS08-013

---

### Vulnerability in Microsoft Office

#### **MS08-013 - Vulnerability in Microsoft Office Could Allow Remote Code Execution**

This critical security update resolves a reported vulnerability in Microsoft Office. The vulnerability could allow remote code execution if a user opens a specially crafted Microsoft Office file with a malformed object inserted into the document.

This security update addresses the vulnerability by modifying the way that Microsoft Office loads documents with inserted objects.

#### **Affected Software**

Microsoft Office 2000 Service Pack 3  
Microsoft Office XP Service Pack 3  
Microsoft Office 2003 Service Pack 2

#### **Vulnerability**

**CVE-2008-0103-** Microsoft Office Execution Jump Vulnerability

#### **Vulnerability Information**

The vulnerability could allow remote code execution if a user opens a specially crafted Microsoft Office document with a malformed object inserted into the document. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

The vulnerability is caused by a memory handling error in Microsoft Office when a user opens a specially crafted Office file with malformed objects inserted. The error may corrupt system memory in such a way that an attacker could execute arbitrary code.

This vulnerability requires that a user open a specially crafted Office file with an affected edition of Microsoft Office.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted Office file to the user and by convincing the user to open the file.

In a Web-based attack scenario, an attacker would have to entice a victim to visit a web site hosting a crafted Office document containing the vulnerability. This includes both malicious web sites and legitimate sites that have been compromised.

#### **Comment / Mitigation**

- The vulnerability cannot be exploited on 2007 Microsoft Office Systems, Microsoft Excel Viewer 2003 Service Pack 3, or Microsoft Word Viewer 2003 Service Pack 3.
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful, a user must open an attachment that is sent in an e-mail message.

#### **References:**

<http://www.microsoft.com/technet/security/bulletin/MS08-013.msp>

---

## Summary of Important Patches

---

---

### Microsoft Security Bulletin – MS08-003

---

#### Vulnerability in Active Directory

##### **MS08-003 Vulnerability in Active Directory Could Allow Denial of Service**

##### **Affected Software**

Microsoft Windows 2000 Service Pack 4

Windows XP Service Pack 2

Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2

Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2

Windows Server 2003 x64 Edition Service Pack 1 and Windows Server 2003 x64 Edition Service Pack 2

Windows Server 2003 x64 Edition Service Pack 1 and Windows Server 2003 x64 Edition Service Pack 2

Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems

##### **Vulnerability**

##### **CVE-2008-0088 - Active Directory Vulnerability**

##### **Vulnerability Information**

A denial of service vulnerability exists in implementations of Active Directory on Microsoft Windows 2000 and Windows Server 2003. The vulnerability also exists in implementations of Active Directory Application Mode (ADAM) when installed on Windows XP and Windows Server 2003. The vulnerability is due to improper validation of specially crafted LDAP requests. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and automatically restart.

##### **Comment / Mitigation**

The vulnerability is caused by the LDAP service performing insufficient checks for specially crafted LDAP requests.

- **Block TCP ports 389 and 3268 at the perimeter firewall**  
These ports are used to initiate a connection with the affected component. Blocking it at the enterprise firewall, both inbound and outbound, will help prevent systems that are behind that firewall from attempts to exploit this vulnerability. We recommend that you block all unsolicited inbound communication from the Internet to help prevent attacks that may use other ports.
- **To help protect from network-based attempts to exploit this vulnerability, block the affected ports by using IPSec on the affected systems.**

##### **References:**

<http://www.microsoft.com/technet/security/bulletin/MS08-003.msp>

---

## Microsoft Security Bulletin – MS08-004

---

### Vulnerability in Windows TCP/IP

#### MS08-004 Vulnerability in Windows TCP/IP Could Allow Denial of Service

#### Affected Software

Windows Vista  
Windows Vista x64 Edition

#### Vulnerability

**CVE-2008-0084** - Vista TCP/IP Vulnerability

#### Vulnerability Information

A denial of service vulnerability exists in TCP/IP processing in Windows Vista. An attacker could exploit the vulnerability by creating a specially crafted DHCP server that returns a specially crafted packet to a host, corrupting TCP/IP structures and causing the affected system to stop responding and automatically restart.

#### Comment / Mitigation

The vulnerability lies in the way that the TCP/IP stack handles packets received from DHCP servers. A victim must be on the same network subnet as the attacker for this vulnerability to be exploited.

It is GovCertUK's opinion that users connecting to untrusted networks (including wireless networks) are at most risk from this vulnerability.

- An attacker can only receive a DHCP request and respond with a specially crafted packet by using a specially crafted DHCP server within the same link or via a DHCP Relay Agent.

#### References:

<http://www.microsoft.com/technet/security/bulletin/MS08-004.mspx>

---

## Microsoft Security Bulletin – MS08-005

---

### Vulnerability in Internet Information Services

#### MS08-005 Vulnerability in Internet Information Services Could Allow Elevation of Privilege

##### Affected Software

Microsoft Windows 2000 Service Pack 4  
Windows XP Service Pack 2  
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2  
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2  
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2  
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems  
Windows Vista  
Windows Vista x64 Edition

##### Vulnerability

**CVE-2008-0074** - File Change Notification Vulnerability

##### Vulnerability Information

A local elevation of privilege vulnerability exists in the way that the Internet Information Service handles file change notifications in the FTPRoot, NNTPFileRoot, and WWWRoot folders. An attacker who successfully exploited this vulnerability could execute arbitrary code in the context of local system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

##### Comment / Mitigation

The vulnerability exists in the way that the Internet Information Service handles the file change notifications in the FTPRoot, NNTPFileRoot, and WWWRoot folders.

Exploitation of this vulnerability would require that the attacker have write access to the FTP root or NNTP root folders. By default the IIS anonymous access account, IUSR\_MACHINENAME, has write access to the FTP root and NNTP root folders. Stopping these services will prevent the FTP and NNTP services from responding to change notifications for files in those directories.

- On Windows XP Service Pack 2 and Windows Server 2003, the IUSR\_MACHINENAME account (used for anonymous access) does not have write access to the WWW root folders by default.
- The specially crafted file or folder that would be required to exploit this vulnerability must be created locally. It could not be created through an FTP client connected to the FTP server service.
- On Windows XP, Windows 2003, and Windows Vista, IIS is not installed or enabled by default.

##### References:

<http://www.microsoft.com/technet/security/bulletin/MS08-005.msp>

---

## Microsoft Security Bulletin – MS08-006

---

### Vulnerability in Internet Information Services

#### **MS08-006 Vulnerability in Internet Information Services Could Allow Remote Code Execution**

#### **Affected Software**

Windows XP Service Pack 2

Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2

Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2

Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2

Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems

#### **Vulnerability**

**CVE-2008-0075** - ASP HTML Encode Vulnerability

#### **Vulnerability Information**

A remote code execution vulnerability exists in the way that Internet Information Services handles HTML-encoded ASP Web pages. An attacker could exploit the vulnerability by passing input to a Web site's ASP page that performs an HTML Encode operation on the input. An attacker who successfully exploited this vulnerability could then perform any actions on the IIS Server with the same rights as the Worker Process Identity (WPI), which by default is configured with Network Service account privileges.

#### **Comment / Mitigation**

The vulnerability is caused by the way that Internet Information Services incorrectly encodes HTML content via the HTML Encode function.

An attacker who successfully exploited this vulnerability could then perform actions on the IIS Server with the same rights as the Worker Process Identity (WPI), which is configured with Network Service account privileges by default. Services configured with Network Service account privileges obtain authenticated user level access, not administrative level access.

IIS servers whose application pool is configured with a WPI that uses an account with administrative privileges could be more seriously impacted than IIS servers whose application pool is configured with the default WPI settings.

- IIS 5.1 is not part of a default install of Windows XP Service Pack 2.
- On supported editions of Windows Server 2003, IIS is not installed or enabled by default.
- On supported editions of Windows Server 2003, if IIS is enabled, ASP is not installed or enabled by default.
- On supported editions of Windows Server 2003, if IIS is enabled and classic ASP is used, an attacker who successfully exploited this vulnerability could only obtain Network Service account privileges by default. By default, Network Service account privileges have the same user rights as the local user.
- ASP.NET is not affected by this vulnerability. Customers who have only ASP.NET installed and not ASP are not at risk from this vulnerability.

**References:**

<http://www.microsoft.com/technet/security/bulletin/MS08-006.msp>

---

## Microsoft Security Bulletin – MS08-011

---

### Vulnerabilities in Microsoft Works File Converter

**MS08-011 Multiple Vulnerabilities in Microsoft Works File Converter could allow Remote Code Execution**

#### **Affected Software**

Microsoft Office 2003 Service Pack 2

Microsoft Office 2003 Service Pack 3

Microsoft Works 8.0

Microsoft Works Suite 2005

#### **Vulnerability**

**CVE-2007-0216** Input Validation Vulnerability

**CVE-2008-0105** File Converter Index Table Vulnerability

**CVE-2008-0108** Field Length Vulnerability

#### **Vulnerability Information**

Remote code execution vulnerabilities exist in Microsoft Works File Converter due to the way that it improperly validates section length headers, section header index table information and various field lengths with the .wps format. An attacker who successfully exploited either of these vulnerabilities could take complete control of an affected system.

#### **Comment / Mitigation**

- **Mitigation set 1 applies**

#### **References:**

<http://www.microsoft.com/technet/security/bulletin/MS08-011.msp>

## Mitigation information and factors

### Mitigation factors – Set 1

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to persuade users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site.
- An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. 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.
- By default, all supported releases of Microsoft Outlook and Microsoft Outlook Express open HTML e-mail messages in the Restricted sites zone. The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing ActiveX controls from being used when reading HTML e-mail. However, if a user clicks on a link within an e-mail they could still be vulnerable to this issue through the Web-based attack scenario.
- By default, Internet Explorer on Windows Server 2003 runs in a restricted mode that is known as [Enhanced Security Configuration](#). This mode sets the security level for the Internet zone to High. This is a mitigating factor for Web sites that you have not added to the Internet Explorer Trusted sites zone.