



---

## Summary of Critical Patches – October 2007

---

---

### Microsoft Security Bulletin - MS07-055

---

#### Vulnerability in Kodak Image Viewer

#### **MS07-055 Vulnerability in Kodak Image Viewer Could Allow Remote Code Execution**

#### **Affected Software**

Microsoft Windows 2000 Service Pack 4  
Microsoft Windows XP Service Pack 2  
Microsoft Windows Server 2003 Service Pack 1 and Service Pack 2

#### **Vulnerability**

An input validation failure allows remote code execution via specially crafted image files with the rights of the logged on user.

#### **Vulnerability Information**

This critical security update resolves a privately reported vulnerability. A remote code execution vulnerability exists in the way that the Kodak Image Viewer (formerly known as Wang Image Viewer) handles specifically crafted images files. The vulnerability could allow an attacker to remotely execute code on the affected system at the privilege level of the user.

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

- Windows XP and Windows Server 2003 systems are only vulnerable if they have been upgraded from Windows 2000.
- When the 'Use Windows Classic Folders' options is enabled in 'Folder Options', users are protected from shell-based attacks.
- If Office 2003 has been installed, the system is not vulnerable as an image viewer application is installed with Office 2003 that takes over the file association.
- 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 convince 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.

## Microsoft Monthly Patch Summary - Date: 12<sup>th</sup> October 2007

---

- 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.

### References:

<http://www.microsoft.com/technet/security/bulletin/ms07-055.mspx>

<http://isc.sans.org/>

---

## Microsoft Security Bulletin - MS07-056

---

### Security Update for Outlook Express and Windows Mail

#### MS07-056 Security Update for Outlook Express and Windows Mail

#### Affected Software

Microsoft Windows 2000 Service Pack 4 with Outlook Express 5.5 Service Pack 2  
Microsoft Windows 2000 Service Pack 4 with Outlook Express 6 Service Pack 1  
Windows XP Service Pack 2 with Microsoft Outlook Express 6  
Windows XP Professional x64 Edition Service Pack 2 with Microsoft Outlook Express 6  
Windows Server 2003 Service Pack 1 with Microsoft Outlook Express 6  
Windows Server 2003 Service Pack 2 with Microsoft Outlook Express 6  
Windows Server 2003 x64 Edition with Microsoft Outlook Express 6  
Windows Server 2003 x64 Edition Service Pack 2 with Microsoft Outlook Express 6  
Windows Server 2003 with SP1 for Itanium-based Systems with Microsoft Outlook Express 6  
Windows Server 2003 with SP2 for Itanium-based Systems with Microsoft Outlook Express 6  
Windows Vista with Windows Mail \*  
Windows Vista x64 Edition with Windows Mail \*

*\* Windows Vista versions with Windows Mail are rated as important rather than critical severity*

#### Vulnerability

An input validation failure in the NNTP protocol allows remote code execution.

#### Vulnerability Information

This critical security update resolves one privately reported vulnerability. The vulnerability could allow remote code execution due to an incorrectly handled malformed NNTP response. An attacker could exploit the vulnerability by constructing a specially crafted Web page. If a user viewed the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged-on user. This security update replaces MS06-076.

#### Comment / Mitigation:

- 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, Web sites that accept or host user-provided content, or compromised Web sites and advertisement servers 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.

## Microsoft Monthly Patch Summary - Date: 12<sup>th</sup> October 2007

---

- Internet Explorer 7 Protect Mode on Microsoft Windows Vista displays a warning dialogue that a Web page is attempting to access Windows Mail. The user would have to click allow before the vulnerability could be exploited.

### References:

<http://www.microsoft.com/technet/security/bulletin/ms07-056.msp>

<http://isc.sans.org/>

---

## Microsoft Security Bulletin - MS07-057

---

### Cumulative Security Update for Internet Explorer

#### MS07-057 Cumulative Security Update for Internet Explorer

#### Affected Software

##### *Internet Explorer 5.01 and Internet Explorer Service Pack 1*

Microsoft Windows 2000 Service Pack 4 with Microsoft Internet Explorer 5.01 Service Pack 4  
Microsoft Windows 2000 Service Pack 4 with Microsoft Internet Explorer 6 Service Pack 1

##### *Internet Explorer 6*

Windows XP Service Pack 2 with Microsoft Internet Explorer 6  
Windows XP Professional x64 Edition and Service Pack 2 with Microsoft Internet Explorer 6  
Windows Server 2003 Service Pack 1 and Service Pack 2 with Microsoft Internet Explorer 6 \*  
Windows Server 2003 x64 Edition and Service Pack 2 with Microsoft Internet Explorer 6 \*  
Windows Server 2003 with Service Pack 1 and Service Pack 2 for Itanium-based Systems with Microsoft Internet Explorer 6 \*

##### *Internet Explorer 7*

Windows XP Service Pack 2 with Windows Internet Explorer 7  
Windows XP Professional x64 Edition and Service Pack 2 with Windows Internet Explorer 7  
Windows Server 2003 Service Pack 1 and Service Pack 2 with Windows Internet Explorer 7 \*  
Windows Server 2003 x64 Edition and Service Pack 2 with Windows Internet Explorer 7 \*  
Windows Server 2003 with Service Pack 1 and Service Pack 2 for Itanium-based Systems with Windows Internet Explorer 7 \*  
Windows Vista with Windows Internet Explorer 7  
Windows Vista x64 Edition with Windows Internet Explorer 7

\* *Rated as moderate rather than critical severity*

#### Vulnerabilities

This critical security update resolves three privately reported vulnerabilities and one publicly disclosed vulnerability. The vulnerability with the most serious security impact could allow remote code execution if a user viewed a specially crafted Web page using Internet Explorer. The security update addresses three vulnerabilities by not allowing the browser window content to persist after navigation has occurred. The update addresses the fourth vulnerability by modifying the script error exception handling so that no attempt is made to access the freed memory. This security update replaces MS07-045.

#### **CVE-2007-3892 - Address Bar Spoofing Vulnerability**

A spoofing vulnerability exists in Internet Explorer that could allow an attacker to display spoofed content in a browser window. The address bar and other parts of the trust UI has been navigated away from the attacker's Web site but the content of the window still contains the attacker's Web page.

#### **CVE-2007-3893 - Error Handling Memory Corruption Vulnerability**

A remote code execution vulnerability exists in Internet Explorer due to an unhandled error in certain situations. An attacker could exploit the vulnerability by constructing a specially crafted

Web page. If a user viewed the Web page, the vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could gain the same user rights as the logged on user.

**CVE-2007-1091 & CVE-2007-3826 - Address Bar Spoofing Vulnerability**

Spoofing vulnerabilities exist in Internet Explorer that could allow an attacker to display spoofed content in a browser window. The address bar and other parts of the trust UI has been navigated away from the attacker's Web site but the content of the window still contains the attacker's Web page.

**Comment / Mitigation:**

- In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's Web site.
- The Restricted sites zone helps reduce attacks that could try to exploit this vulnerability by preventing Active Scripting from being used when reading HTML e-mail messages. However, if a user clicks a link in an e-mail message, they could still be vulnerable to this issue through the Web-based attack scenario.
- By default, all supported versions of Microsoft Outlook and Microsoft Outlook Express open HTML e-mail messages in the Restricted sites zone. The Restricted sites zone helps reduce the number of successful attacks that exploit this vulnerability by preventing Active Scripting and 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 mitigates this vulnerability.

**References:**

<http://www.microsoft.com/technet/security/bulletin/ms07-057.msp>  
<http://isc.sans.org/>

---

## Microsoft Security Bulletin - MS07-060

---

### Vulnerability in Microsoft Word

#### MS07-060 Vulnerability in Microsoft Word Could Allow Remote Code Execution

#### Affected Software

Microsoft Word 2000 Service Pack 3  
Microsoft Word 2002 Service Pack 3 \*  
Microsoft Office 2004 for Mac \*

*\* Rated as important rather than critical severity*

#### Vulnerability

An input validation problem allows remote code execution with the rights of the logged on user.

#### Vulnerability Information

A remote code execution vulnerability exists in the way that Word handles specially crafted Word files. If a user opens a specially crafted Word file with a malformed string it could allow remote code execution at the privilege level of the user.

#### Comment / Mitigation:

- The vulnerability cannot be exploited on the 2007 Microsoft Office system.
- The vulnerability cannot be exploited on Microsoft Office 2003 as a remote code execution. However, Microsoft Office 2003 could exit unexpectedly.
- 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.
- 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.
- 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/ms07-060.mspx>

<http://isc.sans.org/>

---

## Summary of Important Patches

---

---

### Microsoft Security Bulletin - MS07-058

---

#### Vulnerability in RPC

#### MS07-058 Vulnerability in RPC Could Allow Denial of Service

#### Affected Software

Microsoft Windows 2000 Service Pack 4 (replaces MS06-031)  
Windows XP Service Pack 2  
Windows XP Professional x64 Edition  
Windows Server 2003 Service Pack 1 and Service Pack 2  
Windows Server 2003 x64 Edition and Service Pack 2  
Windows Server 2003 with Service Pack 1 and Service Pack 2 for Itanium-based Systems  
Windows Vista  
Windows Vista x64 Edition

#### Vulnerability

NTLMSSP authentication can be abused to cause the RPC service to stop in a way that it also prevents the system from restarting the service.

#### Vulnerability Information

This update resolves a privately reported vulnerability. A denial of service vulnerability exists in the remote procedure call (RPC) facility due to a failure in communicating with the NTLM security provider when performing authentication of RPC requests. An anonymous attacker could exploit the vulnerability by sending a specially crafted RPC authentication request to a computer over the network. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and automatically restart.

#### Comment / Mitigation:

Firewall best practices and standard default firewall configurations can help protect networks from attacks that originate outside the enterprise perimeter. Best practices recommend that systems that are connected to the Internet have a minimal number of ports exposed.

#### References:

<http://www.microsoft.com/technet/security/bulletin/ms07-058.mspx>

<http://isc.sans.org/>

---

## Microsoft Security Bulletin - MS07-059

---

### Vulnerability in Windows SharePoint Services 3.0 and Office SharePoint Server 2007

#### **MS07-059 Vulnerability in Windows SharePoint Services 3.0 and Office SharePoint Server 2007 Could Result in Elevation of Privilege Within the SharePoint Site**

#### **Affected Software**

Windows Server 2003 Service Pack 1 and Service Pack 2 with Microsoft Windows SharePoint Services 3.0

Windows Server 2003 x64 Edition and Service Pack 2 with Microsoft Windows SharePoint Services 3.0

Microsoft Office SharePoint Server 2007

Microsoft Office SharePoint Server 2007 x64 Edition

#### **Vulnerability**

XSS issues on the SharePoint server cause elevate privileges problems on the server itself and information leaks on the client connecting to such server.

#### **Vulnerability Information**

This security update resolves a publicly reported vulnerability in Microsoft Windows SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007. The vulnerability could allow an attacker to run arbitrary script that could result in elevation of privilege within the SharePoint site, as opposed to elevation of privilege within the workstation or server environment. The vulnerability could also allow an attacker to run arbitrary script to modify a user's cache, resulting in information disclosure at the workstation. The security update addresses the vulnerability by modifying the way that Microsoft Windows SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007 validate URL-encoded requests.

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

- In a Web-based attack scenario, Web sites that accept or host user-provided content, or compromised Web sites and advertisement servers 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 contains a specially-crafted URL with embedded Javascript.
- In the information disclosure scenario, clients that have the advanced Internet option 'Do not save encrypted pages to disk' turned on in Internet Explorer, would be protected against cache modification if they have access the site through the Secure Sockets Layer (SSL) protocol.

#### **References:**

<http://www.microsoft.com/technet/security/bulletin/MS07-059.msp>

<http://isc.sans.org/>