



## eSecurity Advisory SEPTEMBER 2006 MICROSOFT SECURITY BULLETIN RELEASE

The purpose of this update is to provide you with a summary of the Microsoft September 2006 Security Bulletin release.

### NEW BULLETINS

Microsoft is releasing the following security bulletins for newly discovered vulnerabilities:

MAXIMUM SEVERITY	BULLETIN NUMBER	PRODUCTS AFFECTED	IMPACT
Important	MS06-052	Microsoft Windows	Remote Code Execution
Moderate	MS06-053	Microsoft Windows	Information Disclosure
Critical	MS06-054	Microsoft Office (Publisher)	Remote Code Execution

Summaries for these new bulletins may be found at:

<http://www.microsoft.com/technet/security/bulletin/ms06-sep.aspx>

---

### RE-RELEASED BULLETINS

In addition, Microsoft is re-releasing the following security bulletin:

MAXIMUM SEVERITY	BULLETIN NUMBER	PRODUCTS AFFECTED (re-release only)	IMPACT
Critical	MS06-040	Microsoft Windows	Remote Code Execution
Critical	MS06-042	Microsoft Windows	Remote Code Execution

Information on this re-released bulletin may be found at the following pages:

<http://www.microsoft.com/technet/security/Bulletin/MS06-040.aspx>

<http://www.microsoft.com/technet/security/Bulletin/MS06-042.aspx>

---

***Customers are advised to review the information in the bulletins, test and deploy the updates immediately in their environments, if applicable.***

Listed below is more technical information that may be helpful to users to protect their work and home computers.

## MS06-052

**Title:** Vulnerability in Pragmatic General Multicast (PGM) Could Allow Remote Code Execution (919007)

**Executive Summary:**

There is a remote code execution vulnerability that could allow an attacker to send a specially crafted multicast message to an affected system and execute code on the affected system. The MSMQ service, which is the Windows service needed to allow PGM communications is not installed by default

**Affected Software:**

- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** **Important**

**Restart Requirement:** You must restart your system after you apply this security update.

**Update Can Be Uninstalled:** Yes. To remove this security update, use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.

**More information on this vulnerability is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS06-052.msp>

---

## MS06-053

**Title:** Vulnerability in Indexing Service Could Allow Cross-Site Scripting (920685)

**Executive Summary:**

There is an information disclosure vulnerability in the Indexing Service because of the way that it handles query validation. The vulnerability could allow an attacker to run client-side script on behalf of a user. The script could spoof content, disclose information, or take any action that the user could take on the affected Web site.

**Affected Software:**

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

**Affected Components:**

- Indexing Service

**Impact of Vulnerability:** Information Disclosure

**Maximum Severity Rating:** **Moderate**

**Restart Requirement:** A system restart is not required after applying this security update.

**Update Can Be Uninstalled:** Yes. To remove this security update, use the Add or Remove Programs tool in Control Panel. System administrators can also use the Spuninst.exe utility to remove this security update.

**More information on this vulnerability is available at:**  
<http://www.microsoft.com/technet/security/bulletin/MS06-053.msp>

---

## MS06-054

**Title:** Vulnerability in Microsoft Publisher Could Allow Remote Code Execution (910729)

### Executive Summary:

A remote code execution vulnerability exists in Publisher. An attacker could exploit this vulnerability when Publisher parses a file with a malformed string.

If a user were logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

### Affected Software:

- Microsoft Office 2000 Service Pack 3
- Microsoft Office XP Service Pack 3
- Microsoft Office 2003 Service Pack 1 and Service Pack 2
- Office Publisher 2000
- Office Publisher 2002
- Office Publisher 2003

### Affected Components:

- Publisher

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** **Critical**

**Restart Requirement:** You must restart your system after you apply this security update.

**Update Can Be Uninstalled:** No.

**More information on this vulnerability is available at:**  
<http://www.microsoft.com/technet/security/bulletin/MS06-054.msp>

---

## MS06-040 (Re-release)

**Title:** Vulnerability in Server Service Could Allow Remote Code Execution (921883)

### Affected Software:

- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

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

**Reason for Re-release:**

This update resolves a privately disclosed vulnerability as well as additional issues discovered through internal investigations. An attacker who successfully exploited the vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** **Critical**

**More information on this vulnerability is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS06-040.msp>

---

**MS06-042 (Re-release)**

**Title:** Cumulative Security Update for Internet Explorer (918899)

**Affected Software:**

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

**Affected Components:**

- Internet Explorer 5.01 Service Pack 4 on Microsoft Windows 2000 Service Pack 4
- Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 4 or on Microsoft Windows XP Service Pack 1
- Internet Explorer 6 for Microsoft Windows XP Service Pack 2
- Internet Explorer 6 for Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Internet Explorer 6 for Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Internet Explorer 6 for Microsoft Windows Server 2003 x64 Edition
- Internet Explorer 6 for Microsoft Windows XP Professional x64 Edition

**Reason for Re-release:**

On August 24, 2006 this Security Bulletin and the Internet Explorer 6 Service Pack 1 security updates were updated to address an issue documented in Microsoft Knowledge Base Article 923762. This issue may lead to an additional buffer overrun condition only affecting Internet Explorer 6 Service Pack 1 customers that have applied the original version of that update released August 8th, 2006. The security issue is documented in the Vulnerability Details section as Long URL Buffer Overflow – CVE-2006-3869. Internet Explorer 6 Service Pack 1 Customers should apply the new update immediately. Microsoft Knowledge Base Article 918899 documents this and any other currently known issues that customers may experience when they install this security update.

**eSecurity Advisory: SEPTEMBER 2006 MICROSOFT SECURITY BULLETIN RELEASE**

Delaware Department of Technology and Information  
September 13, 2006

The article also documents recommended solutions for these issues. For more information, see Microsoft Knowledge Base Article 918899.

**Impact of Vulnerability:** Remote Code Execution

**Maximum Severity Rating:** **Critical**

**More information on this vulnerability is available at:**

<http://www.microsoft.com/technet/security/bulletin/MS06-042.aspx>