



Summary of Critical Patches – May 2008

Microsoft Security Bulletin - MS08-026

Vulnerabilities in Microsoft Word

MS08-026 Vulnerabilities in Microsoft Word Could Allow Remote Code Execution

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

This update addresses critical security flaws in supported editions of Microsoft Word 2000 Service Pack 3, Outlook 2007 and Outlook 2007 Service Pack 1. For all later versions of Word the severity is rated as important.

Affected Software

Microsoft Office 2000 Service Pack 3
Microsoft Office XP Service Pack 3
Microsoft Office 2003 Service Pack 2
Microsoft Office 2003 Service Pack 3
Microsoft Word Viewer 2003
Microsoft Word Viewer 2003 Service Pack 3
Microsoft Word 2007
Microsoft Outlook 2007
Microsoft Word 2007 Service Pack 1
Microsoft Outlook 2007 Service Pack 1
Microsoft Office 2004 for Mac
Microsoft Office 2008 for Mac

Vulnerability Details

CVE-2008-1091

A remote code execution vulnerability exists in the way that Word handles specially crafted Rich Text Format (.rtf) files. It is caused by a memory calculation error when processing a malformed string in a purposely crafted file. The error may corrupt system memory in such a way that an attacker could execute arbitrary code.

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. The attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

CVE-2008-1434

A remote code execution vulnerability exists in the way that Word handles specially crafted Word files. The vulnerability is caused by a memory calculation error when processing CSS values in the crafted Word file. The error may corrupt system memory in such a way that an attacker could execute arbitrary code.

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. The attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Comment / Mitigation

- The update removes the vulnerability described in CVE-2008-1091 by modifying the way Word calculates the required memory allocation when opening .rtf files.
- The update removes the vulnerability described in CVE-2008-1434 by modifying the way Word calculates the required memory allocation when processing CSS values when opening Word files.
- 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.
- Mitigation set 1 and 2 applies.
- There are currently no known exploits for this vulnerability; however GovCertUK recommend this patch is applied immediately.
- See <http://www.microsoft.com/technet/security/bulletin/MS08-026.mspx> for relevant mitigation advice.

References

<http://www.microsoft.com/technet/security/bulletin/MS08-026.mspx>

Microsoft Security Bulletin - MS08-027

Vulnerability in Microsoft Publisher

MS08-027 Vulnerability Microsoft Publisher Could Allow Remote Code Execution

This security update resolves a privately reported vulnerability in Microsoft Publisher that 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.

This security update is rated Critical for Microsoft Publisher 2000 Service Pack 3, and Important for Microsoft Publisher 2002 Service Pack 3, Microsoft Publisher 2003 Service Pack 2, Microsoft Publisher 2003 Service Pack 3, Microsoft Publisher 2007, and Microsoft Publisher 2007 Service Pack 1.

Affected Software

Microsoft Publisher 2000 Service Pack 3
Microsoft Publisher 2002 Service Pack 3
Microsoft Publisher 2003 Service Pack 2
Microsoft Publisher 2003 Service Pack 3
Microsoft Publisher 2007
Microsoft Publisher 2007 Service Pack 1

Vulnerability Details

CVE-2008-0119

The vulnerability is caused by an error calculating object handler data when opening a specially crafted Publisher file. The error may corrupt system memory in such a way that an attacker could execute arbitrary code.

An attacker who successfully exploited this vulnerability could take complete control of an affected system. If a user is logged on with administrative user rights, an attacker could take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Comment / Mitigation

- The update removes the vulnerability described in CVE-2008-0119 by properly validating object handler data when opening Publisher files.
- Mitigation set 1 and 2 applies.
- There are currently no known exploits for this vulnerability; however GovCertUK recommend this patch is applied immediately.
- See <http://www.microsoft.com/technet/security/bulletin/MS08-027.aspx> for relevant mitigation advice.

References

<http://www.microsoft.com/technet/security/bulletin/MS08-027.aspx>

Microsoft Security Bulletin - MS08-028

Vulnerability in Microsoft Jet Database Engine

MS08-028 Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution

This important security update resolves a security vulnerability in the Microsoft Jet Database Engine (Jet) in Windows. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

This is an important security update for the Microsoft Jet 4.0 Database Engine, and it also addresses the vulnerability first described in Microsoft Security Advisory 950627.

Affected Software

Vulnerable versions of Microsoft Jet 4.0 Database Engine, specifically the file 'msjet40.dll' with a version lower than 4.0.9505.0, are present in:

Microsoft Windows 2000 Service Pack 4
Windows XP Service Pack 2
Windows XP Professional x64
Windows Server 2003 Service Pack 1
Windows Server 2003 x64
Windows Server 2003 with SP1 for Itanium

Vulnerability Details

CVE-2007-6026

An attacker could exploit the buffer overrun vulnerability in Jet, by creating a specially crafted database query and sending it through an application that uses Jet. Exploiting this vulnerability would allow an attacker to remotely execute code with the privileges of the current user, and gain complete control of the system. Upon gaining control, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability via email, the attacker would either need to convince the user to open the attached Word file contain the exploit, or in Outlook 2007, view the document in HTML in the preview pane.

Comment / Mitigation

- This security update addresses the vulnerability by modifying the way that the Microsoft Jet Database Engine parses data within a database.
- Systems with Microsoft Outlook can mitigate the HTML email vector for Outlook 2007 by configuring mail to be read in plain text only.
- Mitigation set 1 applies.
- Systems running all supported editions of Windows XP Service Pack 3, Windows Server 2003 Service Pack 2, Windows Vista, and Windows Server 2008 are not affected by this vulnerability.

- See <http://www.microsoft.com/technet/security/bulletin/MS08-028.aspx> for relevant mitigation advice.

References

<http://www.microsoft.com/technet/security/advisory/950627.aspx>
<http://www.microsoft.com/technet/security/bulletin/MS08-28.aspx>

Summary of Moderate Patches

Microsoft Security Bulletin - MS08-029

Vulnerability in Microsoft Security Software

MS08-029 Vulnerability in Microsoft Malware Protection Engine Could Allow Denial of Service

This security update resolves two reported vulnerabilities in the Microsoft Malware Protection Engine. The vulnerabilities could be exploited using specially crafted files. When the target computer receives the files and the Microsoft Malware Protection Engine scans them, a denial of service would occur. If successfully exploited it would cause the computer to stop responding and automatically restart.

The Microsoft Malware Protection Engine is part of various pieces of Microsoft software; the severity of this flaw differs for each package. The security update is rated moderate for Windows Live OneCare, Microsoft Antigen for Exchange, Microsoft Antigen for SMTP Gateway, Microsoft Windows Defender, Microsoft Forefront Client Security, Microsoft Forefront Security for Exchange Server, and Microsoft Forefront Security for SharePoint. The security update is rated as low for Standalone System Sweeper located in Diagnostics and Recovery Toolset 6.0.

The security update addresses the vulnerability by modifying the way that the Malware Protection Engine processes files.

Affected Software

Severity Rated Moderate

Windows Live OneCare
Microsoft Antigen for Exchange
Microsoft Antigen for SMTP Gateway
Microsoft Windows Defender
Microsoft Forefront Client Security
Microsoft Forefront Security for Exchange Server
Microsoft Forefront Security for SharePoint

Severity Rated Low

Standalone System Sweeper located in Diagnostics and Recovery Toolset 6.0

Vulnerability Details

CVE-2008-1437

A denial of service vulnerability exists in the Microsoft Malware Protection Engine because of the way that it processes specially crafted files. An attacker could exploit the vulnerability by constructing a specially crafted file that could allow a denial of service when the target computer system receives, and the Microsoft Malware Protection Engine scans, the file. An attacker who successfully exploited this vulnerability could cause the computer to stop responding and automatically restart.

CVE-2008-1438

A denial of service vulnerability exists in the Microsoft Malware Protection Engine because of the way that it processes specially crafted files. An attacker could exploit the vulnerability by constructing a specially crafted file that could allow a denial of service when the target computer system receives, and the Microsoft Malware Protection Engine scans, the file. An attacker who successfully exploited this vulnerability could lead to a disk-space exhaustion denial of service condition.

Comment / Mitigation

- There is no relevant mitigation advice for this advisory.
- See <http://www.microsoft.com/technet/security/bulletin/MS08-029.msp> for relevant mitigation advice.

References

<http://www.microsoft.com/technet/security/bulletin/MS08-29.msp>

Mitigation Information and factors

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

Mitigation factors – Set 1

- 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 could contain specially crafted content that could exploit this vulnerability. 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 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.

Mitigation factors – Set 2

- 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.