



Summary of Critical Patches – March 2008

Microsoft Security Bulletin - MS08-014

Vulnerability in Microsoft Excel

MS08-014 Vulnerability in Microsoft Excel Could Allow Remote Code Execution

This security update resolves several privately reported and publicly reported vulnerabilities in Microsoft Office Excel that could allow remote code execution if a user opens a specially crafted Excel file. 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.

Affected Software

Microsoft Office Excel 2000 Service Pack 3
Microsoft Office Excel 2002 Service Pack 3
Microsoft Office Excel 2003 Service Pack 2
Microsoft Office Excel Viewer 2003
Microsoft Office Excel 2007
Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats
Microsoft Office 2004 for Mac
Microsoft Office 2008 for Mac

Vulnerability Details

CVE-2008-0111

A remote code execution vulnerability exists in the way Excel processes data validation records when loading Excel files into memory.

An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

CVE-2008-0112

A remote code execution vulnerability exists in the way Excel handles data when importing files into Excel.

An attacker could exploit the vulnerability by importing a malformed .slk file into Excel from an attacker which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

CVE-2008-0114

A remote code execution vulnerability exists in the way Excel handles Style record data when opening Excel file.

An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

CVE-2008-0115

A remote code execution vulnerability exists in the way Excel handles malformed formulas.

An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

CVE-2008-0116

A remote code execution vulnerability exists in the way Excel handles rich text values when loading application data into memory.

An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

CVE-2008-0117

A remote code execution vulnerability exists in the way Excel handles conditional formatting values.

An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

CVE-2008-0081

A remote code execution vulnerability exists in the way Excel handles macros when opening specially crafted Excel files.

An attacker could exploit the vulnerability by sending a malformed file which could be hosted on a specially crafted or compromised Web site, or included as an e-mail attachment.

Comment / Mitigation

- Mitigation set 1 applies
- 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.
- See <http://www.microsoft.com/technet/security/bulletin/MS08-014.mspx> for relevant mitigation advice.

Comment / Mitigation for CVE-2008-0081

Advice is as above, except:

- The vulnerability had been publicly exposed when the original security bulletin was written. This vulnerability was first described in [Microsoft Security Advisory 947563](#).
- It is known that this vulnerability is being **actively exploited**.
- GovCertUK strongly recommend that you apply this update as soon as possible.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-014.mspx>

Microsoft Security Bulletin - MS08-015

Vulnerability in Microsoft Outlook

MS08-015 Vulnerability in Microsoft Outlook Could Allow Remote Code Execution

This security update resolves a privately reported vulnerability in Microsoft Office Outlook. The vulnerability could allow remote code execution if Outlook is passed a specially crafted mailto URI. An attacker who successfully exploited these vulnerabilities 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.

Affected Software

Microsoft Office Outlook 2000 Service Pack 3
Microsoft Office Outlook XP Service Pack 3
Microsoft Office Outlook 2003 Service Pack 2
Microsoft Office Outlook 2003 Service Pack 3
Microsoft Office Outlook 2007

Vulnerability Details

CVE-2008-0110

A remote code execution vulnerability exists in the way Outlook handles "mailto" URIs that could allow an attacker to read and control a user's e-mail account.

An attacker could exploit the vulnerability by convincing a user to visit a specially crafted Web page. An attacker could then read a user's existing e-mail messages and potentially redirect all future messages to an attacker-controlled system.

Comment / Mitigation

- Mitigation set 1 applies
- The vulnerability cannot be exploited automatically through e-mail. For an attack to be successful, a user must open an e-mail message that contains a specially crafted mailto URI and click on the mailto link.
- This vulnerability is not exploitable by simply viewing an e-mail through the Outlook preview pane.
- See <http://www.microsoft.com/technet/security/bulletin/MS08-015.mspx> for relevant mitigation advice.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-015.mspx>

Microsoft Security Bulletin - MS08-016

Vulnerabilities in Microsoft Office

MS08-016 Vulnerabilities in Microsoft Office Could Allow Remote Code Execution

This critical security update resolves two privately reported vulnerabilities in Microsoft Office that could allow remote code execution if a user opens a malformed Office file. 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.

Affected Software

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

Vulnerability Details

CVE-2008-0113

A remote code execution vulnerability exists in the way Microsoft Office handles specially crafted Excel files.

An attacker could exploit the vulnerability by creating a malformed file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

CVE-2008-0118

A remote code execution vulnerability exists in the way Microsoft Office processes malformed Office files.

An attacker could exploit the vulnerability by creating a malformed file that could be included as an e-mail attachment, or hosted on a specially crafted or compromised Web site.

Comment / Mitigation

- Mitigation set 1 applies
- 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.
- See <http://www.microsoft.com/technet/security/bulletin/MS08-016.mspx> for relevant mitigation advice.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-016.mspx>

Microsoft Security Bulletin - MS08-017

Vulnerability in Microsoft Office Web Components

MS08-017 Vulnerabilities in Microsoft Office Web Components Could Allow Remote Code Execution

This critical update resolves two privately reported vulnerabilities. These vulnerabilities could allow remote code execution if a user viewed a specially crafted Web page or clicked a specially crafted link. 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.

Affected Software

Microsoft Office 2000 Service Pack 3
Microsoft Office XP Service Pack 3
Visual Studio .NET 2002 Service Pack 1
Visual Studio .NET 2003 Service Pack 1
Visual Studio .NET 2003 Service Pack 1
Microsoft BizTalk Server 2002
Microsoft Commerce Server 2000
Internet Security and Acceleration Server 2000 Service Pack 2

Vulnerability Details

CVE-2006-4695

A remote code execution vulnerability exists in the way Microsoft Office Web Components manages memory resources when parsing specially crafted URLs.

An attacker could exploit the vulnerability by constructing a specially crafted Web page.

CVE-2007-1201

Remote code execution vulnerabilities exist in the way Microsoft Office Web Components manages memory resources.

An attacker could exploit the vulnerability by constructing a specially crafted Web page.

Comment / Mitigation

- Mitigation set 1 applies
- 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

Microsoft Monthly Patch Summary - Date: 11th March 2008

the Internet Explorer Trusted sites zone. See the FAQ section of this security bulletin for more information about Internet Explorer Enhanced Security Configuration.

- See <http://www.microsoft.com/technet/security/bulletin/MS08-017.msp> for relevant mitigation advice.

References:

<http://www.microsoft.com/technet/security/bulletin/MS08-017.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:

- There are currently no known exploits for this vulnerability; however GovCertUK recommend this patch be applied at the earliest opportunity.
- In a Web-based attack scenario, an attacker could host a Web page that would 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 each case, social engineering would be required 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.
- Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrator rights.