

RE: OT – 5 New Critical Updates for WinXPSP1 from Windows Update

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6_outlookexpress.stationery/

- *From:* bcwitt <bcwitt@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 13 Sep 2005 05:37:10 -0700
-

Can anybody help me regarding Outlook express? When I try to delete a message I get locked up and have to shut down Outlook. I haven't been able to delete for a few days.
Thanks

"Greg Campbell" wrote:

- > This is the second Tuesday of the month when MS releases the monthly Updates. I'm about to install them.
- >
- > --
- > Greg Campbell
- > computerpotatoZZZ@xxxxxxxxxxxxxxxx
- >
- > =====
- > =====
- > Microsoft Security Bulletin MS04-018
- > Cumulative Security Update for Outlook Express (823353)
- >
- > Issued: July 13, 2004
- > Version: 1.0
- >
- > Summary
- > Who should read this document: Customers who use Microsoft® Outlook Express®
- >
- > Impact of Vulnerability: Denial of Service
- >
- > Maximum Severity Rating: Moderate
- >
- > Recommendation: Customers should consider applying the security update.
- >
- > Security Update Replacement: This bulletin replaces MS04-013: Cumulative Update for Outlook Express and any prior Cumulative Security Updates for Outlook Express.
- >
- > Caveats: None
- >
- > Tested Software and Security Update Download Locations:

RE: OT – 5 New Critical Updates for WinXPSP1 from Windows Update

- >
- > Affected Software:
- >
- > . Microsoft Windows NT® Workstation 4.0 Service Pack 6a
- >
- > . Microsoft Windows NT Server 4.0 Service Pack 6a
- >
- > . Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- >
- > . Microsoft Windows 2000 Service Pack 2, Microsoft Windows 2000 Service Pack 3, Microsoft Windows 2000 Service Pack 4
- >
- > . Microsoft Windows XP and Microsoft Windows XP Service Pack 1
- >
- > . Microsoft Windows XP 64–Bit Edition Service Pack 1
- >
- > . Microsoft Windows XP 64–Bit Edition Version 2003
- >
- > . Microsoft Windows ServerT 2003
- >
- > . Microsoft Windows Server 2003 64–Bit Edition
- >
- > . Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me) – Review the FAQ section of this bulletin for details about these operating systems.
- >
- >
- > Affected Components:
- >
- > . Microsoft Outlook Express 5.5 Service Pack 2: Download the Update
- >
- > . Microsoft Outlook Express 6: Download the Update
- >
- > . Microsoft Outlook Express 6 Service Pack 1: Download the Update
- >
- > . Microsoft Outlook Express 6 Service Pack 1 (64 bit Edition): Download the Update
- >
- > . Microsoft Outlook Express 6 on Windows Server 2003: Download the Update
- >
- > . Microsoft Outlook Express 6 on Windows Server 2003 (64 bit edition): Download the Update
- >
- >
- > The software in this list has been tested to determine if the versions are affected. Other versions either no longer include security update support or may not be affected. To determine the support lifecycle for your product and version, visit the following Microsoft Support Lifecycle Web site.
- >
- > Top of section
- > General Information
- > Executive Summary
- >
- > Executive Summary:
- >

RE: OT – 5 New Critical Updates for WinXPSP1 from Windows Update

- > This update resolves a public vulnerability. A denial of service vulnerability exists in Outlook Express because of a lack of robust verification for malformed e-mail headers. The vulnerability is documented in the Vulnerability Details section of this bulletin. This update also changes the default security settings for Outlook Express 5.5 Service Pack 2 (SP2). This change is documented in the Frequently Asked Questions related to this security update section of this bulletin.
- >
- > If a user is running Outlook Express and receives a specially crafted e-mail message, Outlook Express would fail. If the preview pane is enabled, the user would have to manually remove the message, and then restart Outlook Express to resume functionality.
- >
- > We recommend that customers consider applying the security update.
- >
- > Severity Ratings and Vulnerability Identifiers:
- >
- > Vulnerability Identifiers Impact of Vulnerability Outlook Express 5.5 SP2 Outlook Express 6 Outlook Express 6 SP1 Outlook Express 6 (64 bit Edition) Outlook Express 6 for Windows Server 2003 Outlook Express 6 Windows Server 2003 (64-bit Edition)
- > Malformed E-mail Header Vulnerability – CAN-2004-0215
- > Denial of Service
- > None
- > Moderate
- > None
- > None
- > None
- > None
- > None
- >
- >
- > This assessment is based on the types of systems that are affected by the vulnerability, their typical deployment patterns, and the effect that exploiting the vulnerability would have on them.
- >
- > Top of section
- > Frequently asked questions (FAQ) related to this security update
- >
- > What updates does this release replace?
- > This is a cumulative update that includes the functionality of all the previously-released updates for Outlook Express 5.5 and Outlook Express 6. The security bulletin ID and operating systems that are affected for the previous Outlook Express update are listed in the following table.
- >
- > Bulletin ID Outlook Express 5.5 SP2 Outlook Express 6 Outlook Express 6 SP1 Outlook Express 6 (64 bit Edition) Outlook Express 6 for Windows Server 2003 Outlook Express 6 Windows Server 2003 (64-bit Edition)
- > MS04-013
- > Replaced
- > Replaced
- > Replaced
- > Replaced
- > Replaced
- > Replaced
- >
- >
- > Does this update contain any other changes to functionality?

RE: OT – 5 New Critical Updates for WinXPSP1 from Windows Update

- > Yes. In addition to the change that is listed in the Vulnerability Details section of this bulletin, this update includes the following changes in functionality:
 - >
 - > . Sets Outlook Express 5.5 SP2 to view HTML e-mail messages in the Restricted Sites zone.
 - >
 - > . Fixes a behavior that was introduced in MS03-014 where Outlook Express 6 SP1 and later creates a copy of the Windows Address Book in a predictable location with a file name of "~". After you install this update, Outlook Express will no longer create this copy of the Windows Address Book in a predictable location.
 - >
 - >
 - > How does the extended support for Windows 98, Windows 98 Second Edition, and Windows Millennium Edition affect the release of security updates for these operating systems?
 - > Microsoft will only release security updates for critical security issues. Non-critical security issues are not offered during this support period. For more information about the Microsoft Support Lifecycle policies for these operating systems, visit the following Web site.
 - >
 - > For more information about severity ratings, visit the following Web site.
 - >
 - > Are Windows 98, Windows 98 Second Edition, or Windows Millennium Edition critically affected by any of the vulnerabilities that are addressed in this security bulletin?
 - > No. None of these vulnerabilities are critical in severity on Windows 98, on Windows 98 Second Edition, or on Windows Millennium Edition.
 - >
 - > I'm still using Microsoft Windows NT 4.0 Workstation Service Pack 6a or Windows 2000 Service Pack 2, but extended security update support ended on June 30, 2004. However, this bulletin has a security update for these operating system versions. Why is that?
 - > Windows NT 4.0 Workstation Service Pack 6a and Windows 2000 Service Pack 2 have reached the end of their life cycles as previously documented, and Microsoft extended this support to June 30, 2004. However, the end-of-life for the extended support period occurred very recently. In this case, the majority of the steps that are required to address this vulnerability were completed before June 30, 2004. Therefore, we have decided to release security updates for these operating system versions as part of this security bulletin. We do not anticipate doing this for future vulnerabilities affecting these operating system versions, but we reserve the right to produce updates and to make these updates available when necessary.
 - >
 - > It should be a priority for customers who have these operating system versions to migrate to supported versions to prevent potential exposure to future vulnerabilities. For more information about the Windows Product Life Cycle, visit the following Microsoft Support Lifecycle Web site. For more information about the extended security update support period for these operating system versions, visit the following Microsoft Product Support Services Web site.
 - >
 - > Customers who require additional support for Windows NT Workstation 4.0 SP6a must contact their Microsoft account team representative, their Technical Account Manager, or the appropriate Microsoft partner representative for custom support options. Customers without an Alliance, Premier, or Authorized Contract can contact their local Microsoft sales office. For contact information, visit the Microsoft Worldwide Information Web site, select the country, and then click Go to see a list of phone numbers. When you call, ask to speak with the local Premier Support sales manager.
 - >
 - > For more information, see the Windows Operating System FAQ.
 - >
 - > I just scanned my system by using the Microsoft Baseline Security Analyzer (MBSA) and it did not tell me that I had to install this update. Am I at risk?

RE: OT – 5 New Critical Updates for WinXPSP1 from Windows Update

- > MBSA does not currently scan for Outlook Express–related security updates. However, Windows Update will successfully detect and install this update if it is required. For more information about MBSA and the products that MBSA currently scans, visit the following Microsoft Web site.
- >
- > Can I use Systems Management Server (SMS) to determine if this update is required?
- > No. SMS uses MBSA for detection and this update is not detected by MBSA. However, the registry key information that is available in this bulletin can also be used to write specific file and registry key collection queries in SMS to detect vulnerable systems. For information about how to deploy updates not supported by MBSA with SMS, please review Knowledge Base article 867832 or visit the SMS Web site.
- >
- > Top of section
- > Vulnerability Details
- >
- > Malformed E–mail Header Vulnerability – CAN–2004–0215:
- >
- > A denial of service vulnerability exists that could allow an attacker to send a specially crafted e–mail message causing Outlook Express to fail.
- >
- > Mitigating Factors for Malformed E–mail Header Vulnerability – CAN–2004–0215:
- >
- > . The following versions of Outlook Express are not affected by this vulnerability:
- >
- > . Microsoft Outlook Express 5.5SP2
- >
- > . Microsoft Outlook Express 6 SP1
- >
- > . Microsoft Outlook Express 6 SP1 (64–Bit Edition)
- >
- > . Microsoft Outlook Express 6 on Windows Server 2003
- >
- > . Microsoft Outlook Express 6 on Windows Server 2003 (64–Bit Edition)
- >
- >
- > . If the preview pane is not enabled, the malicious e–mail message would have to be opened by the user for Outlook Express to fail.
- >
- >
- > Top of section
- > Workarounds for Malformed E–mail Header Vulnerability – CAN–2004–0215:
- >
- > Disable the preview pane
- >
- > Disabling the preview pane will prevent the malicious e–mail message from causing Outlook Express to fail on each restart. To disable the preview pane, follow these steps:
- >
- > 1.
- > In Outlook Express, click View, and then click Layout.
- >
- > 2.
- > Click to clear the Show Preview Pane check box, and then click OK.
- >

RE: OT – 5 New Critical Updates for WinXPSP1 from Windows Update

- >
- > Top of section
- > FAQ for Malformed E-mail Header Vulnerability – CAN-2004-0215:
- >
- > What is the scope of the vulnerability?
- > This is a denial of service vulnerability. An attacker who exploited this vulnerability could cause Outlook Express to fail. A user would have to manually remove the e-mail message, and then restart Outlook Express to restore functionality.
- >
- > What causes the vulnerability?
- > The method used by Outlook Express to validate malformed e-mail headers.
- >
- > What is an e-mail header?
- > Mail servers and clients must have information that tells them how to process incoming and outgoing e-mail messages. This information is provided in header fields within the e-mail message. Examples of the type of information that is contained in e-mail header fields include the sender's e-mail address, the recipient's e-mail addresses, the time that the e-mail was sent, and the name of the mail server that received the e-mail message.
- >
- > What might an attacker use the vulnerability to do?
- > An attacker who successfully exploited this vulnerability could cause Outlook Express to fail unexpectedly.
- >
- > Who could exploit the vulnerability?
- > Any user who could deliver a specially crafted message to the affected user's e-mail account could attempt to exploit this vulnerability.
- >
- > How could an attacker exploit the vulnerability?
- > An attacker could exploit the vulnerability by creating a specially crafted e-mail message, and then sending the message to an affected user's e-mail account. If the affected user opens the message, it could cause Outlook Express to fail.
- >
- > I have the preview pane enabled. How can I remove the malicious e-mail message without Outlook Express failing when it starts?
- > You can disable the preview pane without starting Outlook Express by editing the registry. The following steps demonstrate how to disable the preview pane in Outlook Express:
- >
- > Note Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.
- >
- > For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or view the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe.
- >
- > Note We recommend backing up the registry before you edit it.
- >
- > 1.
- > Click Start, click Run, type "regedt32" (without the quotation marks), and then click OK.
- >
- > 2.
- > In Registry Editor, locate the following registry key:

RE: OT – 5 New Critical Updates for WinXPSP1 from Windows Update

- >
- > HKCU\Identities\{Identity GUID}\Software\Microsoft\Outlook Express\5.0\Mail\
- >
- > 3.
- > Click the ShowHybridView data value, click Edit, and change the DWORD value to 0.
- >
- > 4.
- > Click OK and then restart Outlook Express.
- >
- >
- > Information on how to modify the registry is available in Microsoft Knowledge Base article 256986.
- >
- > What systems are primarily at risk from the vulnerability?
- > Systems where Outlook Express 6.0 is used to read e-mail messages, such as workstations and terminal servers, are primarily at risk from this vulnerability.
- >
- > What does the update do?
- > The update removes the vulnerability by modifying the way that Outlook Express validates e-mail headers.
- >
- > When this security bulletin was issued, had this vulnerability been publicly disclosed?
- > Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CAN-2004-0215.
- >
- > When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?
- > No. Microsoft had seen examples of proof of concept code published publicly but had not received any information indicating that this vulnerability had been publicly used to attack customers when this security bulletin was originally issued.
- >
- > Does applying this security update help protect customers from the code that has been published publicly that attempts to exploit this vulnerability?
- > Yes. This security update addresses the vulnerability that is currently being exploited. The vulnerability that has been addressed has been assigned the Common Vulnerability and Exposure number CAN-2004-0215.
- >
- > Top of section
- > Top of section
- > Top of section
- > Security Update Information
- >
- > Prerequisites
- >
- > Microsoft has tested the versions of Windows and the versions of Outlook Express that are listed in this bulletin to assess whether they are affected by this vulnerability and to confirm that the update that this bulletin describes addresses this vulnerability.
- >
- > To install the Outlook Express 6 Service Pack 1 (SP1) versions of this update, you must be running Internet Explorer 6 SP1 (version 6.00.2800.1106) on one of the following versions of Windows:
- >
- > . Microsoft Windows NT Workstation 4.0 Service Pack 6a
- >
- > . Microsoft Windows NT Server 4.0 Service Pack 6a

RE: OT – 5 New Critical Updates for WinXPSP1 from Windows Update

- >
- > . Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6
- >
- > . Microsoft Windows 2000 Service Pack 2, Service Pack 3, or Service Pack 4
- >
- > . Microsoft Windows XP
- >
- > . Microsoft Windows XP Service Pack 1
- >
- > . Microsoft Windows XP 64–Bit Edition Service Pack 1
- >
- >
- > To install the Outlook Express 6 for Windows Server 2003 versions of this update, you must be running Internet Explorer 6 (version 6.00.3790.0000) on Windows Server 2003 (32–bit or 64–bit), or you must be running Internet Explorer 6 (version 6.00.3790.0000) on Windows XP 64–Bit Edition Version 2003.
- >
- > To install the Outlook Express 6 version of this update, you must be running Internet Explorer 6 (version 6.00.2600.0000) on a 32–bit version of Windows XP.
- >
- > . Internet Explorer 5.01 Service Pack 4 (version 5.00.3700.1000) on Windows 2000 SP4
- >
- > . Internet Explorer 5.01 Service Pack 3 (version 5.00.3502.1000) on Windows 2000 SP3
- >
- > . Internet Explorer 5.5 Service Pack 2 (version 5.50.4807.2300) Windows Millennium Edition
- >
- >
- > Versions of Windows, versions of Outlook Express, and versions of Internet Explorer that are not listed in this article are no longer supported. Although you can install some of the update packages that are described in this article on these versions of Windows and on these versions of Outlook Express, Microsoft has not tested these versions to assess whether they are affected by this vulnerability or to confirm that the update that this bulletin describes addresses this vulnerability. We recommend that you upgrade to a supported version of Windows and to a supported version of Outlook Express, and then apply the appropriate update.
- >
- > For more information about how to determine the version of Internet Explorer that you are running, see Microsoft Knowledge Base Article 164539.
- >
- > For more information about support lifecycles for Windows components, visit the following Microsoft Support Lifecycle Web site.
- >
- > For more information about how to obtain the latest service pack for Internet Explorer 6, see Microsoft Knowledge Base Article 328548.
- >
- > For more information about how to obtain the latest service pack for Internet Explorer 5.5, see Microsoft Knowledge Base Article 276369.
- >
- > For more information about how to obtain the latest service pack for Internet Explorer 5.01, see Microsoft Knowledge Base Article 267954.
- >
- > Restart Requirements
- >
- > In some cases, this update does not require a restart. The installer stops the required services, applies the

RE: OT – 5 New Critical Updates for WinXPSP1 from WIndows Update

update, and then restarts the services. However, if the required services cannot be stopped for any reason or if required files are in use, this update will require a restart. If this occurs, a message appears that advises you to restart.

>

> The Windows Server 2003 versions of this security update (including Windows XP 64–Bit Edition Version 2003) support the following setup switches:

>

> /help Displays the command line options

.

• *Follow-Ups:*

◆ ***Re: OT – 5 New Critical Updates for WinXPSP1 from WIndows Update***

◇ *From:* Greg Campbell

• Prev by Date: ***Re: Stationary***

• Next by Date: ***Re: Saving addresses into Stationery***

• Previous by thread: ***Stationary***

• Next by thread: ***Re: OT – 5 New Critical Updates for WinXPSP1 from WIndows Update***

• Index(es):

◆ ***Date***

◆ ***Thread***