

# Microsoft Security Bulletin MS04-018 – Cumulative Security Update for Outlook Express (823353)

**Source:**

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6\\_outlookexpress/2004-07/2](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6_outlookexpress/2004-07/2)

---

**From:** Emily F [MSFT] ([emilyf\\_at\\_onliner.microsoft.com](mailto:emilyf_at_onliner.microsoft.com))

**Date:** 07/13/04

Date: Tue, 13 Jul 2004 12:25:45 -0700

MS04-018 – Cumulative Security Update for Outlook Express (823353)

<http://www.microsoft.com/technet/security/bulletin/ms04-018.msp>

Microsoft Security Bulletin MS04-018  
Cumulative Security Update for Outlook Express (823353)

Issued: July 13, 2004

Version: 1.0

**Executive Summary:**

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.

**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 Security Update for Outlook Express and any prior Cumulative Security Updates for Outlook Express.

**Caveats:** None

**Tested Software and Security Update Download Locations:**

**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.