

# US-CERT Technical Cyber Security Alert TA04-196A -- Multiple Vulnerabilities in Microsoft Windows Components and Outlook Express

*Source:* <http://www.derkeiler.com/Mailing-Lists/Cert/2004-07/0002.html>

---

*From:* CERT Advisory ([cert-advisory\\_at\\_cert.org](mailto:cert-advisory_at_cert.org))

*Date:* 07/14/04

Date: Wed, 14 Jul 2004 16:50:51 -0400

To: [cert-advisory@cert.org](mailto:cert-advisory@cert.org)

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

National Cyber Alert System  
Technical Cyber Security Alert TA04-196A

Multiple Vulnerabilities in Microsoft Windows Components and Outlook Express

Original release date: July 14, 2004

Last revised: --

Source: US-CERT

Systems Affected

\* Microsoft Windows Systems

Overview

Microsoft has released a Security Bulletin Summary for July, 2004. This summary includes several bulletins that address vulnerabilities in various Windows applications and components. Exploitation of some vulnerabilities can result in the remote execution of arbitrary code by a remote attacker. Details of the vulnerabilities and their impacts are provided below.

I. Description

The table below provides a reference between Microsoft's Security Bulletins and the related US-CERT Vulnerability Notes. More information related to the vulnerabilities is available in these documents.

---

Format:

Microsoft Security Bulletin

Related US-CERT Vulnerability Note(s)

---

MS04-024: Vulnerability in Windows Shell Could Allow Remote Code Execution (839645)

VU#106324 Microsoft Windows contains a vulnerability in the way the Windows Shell launches applications

---

MS04-023: Vulnerability in HTML Help Could Allow Code Execution (840315)

VU#187196 Microsoft Windows fails to properly process showHelp URLs

VU#920060 Microsoft Windows HTML Help component fails to properly validate input data

---

MS04-022: Vulnerability in Task Scheduler Could Allow Code Execution (841873)

VU#228028 Microsoft Windows Task Scheduler Buffer Overflow

---

MS04-021: Security Update for IIS 4.0 (841373)

VU#717748 Microsoft Internet Information Server (IIS) 4.0 contains a buffer overflow in the redirect function

---

MS04-020: Vulnerability in POSIX Could Allow Code Execution (841872)

VU#647436 Microsoft Windows contains a buffer overflow in the POSIX subsystem

---

MS04-019: Vulnerability in Utility Manager Could Allow Code Execution (842526)

VU#868580 Microsoft Windows Utility Manager launches applications with system privileges

---

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

VU#869640 Microsoft Outlook Express fails to properly validate malformed e-mail headers

---

## II. Impact

A remote, unauthenticated attacker may exploit VU#717748 to execute arbitrary code on an IIS 4.0 system.

Exploitation of VU#106324, VU#187196, VU#920060, and VU#228028, would permit a remote attacker to execute arbitrary code with the privileges of the current user. The attacker would have to convince a victim to view an HTML document (web page, HTML email) or click on a crafted URI link.

Vulnerabilities described in VU#647436 and VU#868580 permit a local user to gain elevated privileges on the local system.

Exploitation of VU#869640 can lead to a denial-of-service condition against Outlook Express.

## III. Solution

### Apply a patch

Microsoft has provided the patches for these vulnerabilities in the Security Bulletins and on Windows Update.

### Do not follow unsolicited links

It is generally a good practice not to click on unsolicited URLs received in email, instant messages, web forums, or Internet relay chat (IRC) channels. However, this practice does not always prevent exploitation of these types vulnerabilities. For example, a trusted web site could be compromised and modified to deliver exploit script to unsuspecting clients.

### Maintain updated anti-virus software

Anti-virus software with updated virus definitions may identify and prevent some exploit attempts, but variations of exploits or attack vectors may not be detected. Do not rely solely on anti-virus software to defend against these vulnerabilities. More information about viruses and anti-virus vendors is available on the US-CERT Computer Virus Resources page.

## Appendix A. Vendor Information

Specific information about these issue are available in the Security Bulletin Summary for July, 2004 and the US-CERT Vulnerability Notes.

## Appendix B. References

- \* Microsoft's Security Bulletin Summary for July, 2004 –  
<<http://www.microsoft.com/technet/security/bulletin/ms04-jul.msp>>
- \* US-CERT Vulnerability Note VU#106324 –  
<<http://www.kb.cert.org/vuls/id/106324>>
- \* US-CERT Vulnerability Note VU#187196 –  
<<http://www.kb.cert.org/vuls/id/187196>>
- \* US-CERT Vulnerability Note VU#920060 –  
<<http://www.kb.cert.org/vuls/id/920060>>
- \* US-CERT Vulnerability Note VU#228028 –  
<<http://www.kb.cert.org/vuls/id/228028>>
- \* US-CERT Vulnerability Note VU#717748 –  
<<http://www.kb.cert.org/vuls/id/717748>>
- \* US-CERT Vulnerability Note VU#647436 –  
<<http://www.kb.cert.org/vuls/id/647436>>
- \* US-CERT Vulnerability Note VU#868580 –  
<<http://www.kb.cert.org/vuls/id/868580>>
- \* US-CERT Vulnerability Note VU#869640 –  
<<http://www.kb.cert.org/vuls/id/869640>>
- \* Increase Your Browsing and E-Mail Safety –  
<<http://www.microsoft.com/security/incident/settings.msp>>
- \* Working with Internet Explorer 6 Security Settings –  
<<http://www.microsoft.com/windows/ie/using/howto/security/settings.msp>>

---

This alert was created by Jason A. Rafail. Feedback can be directed to the Vulnerability Note authors: Jason A. Rafail, Jeff P. Lanza, Chad R. Dougherty, Damon G. Morda, and Art Manion.

---

This document is available from:

<<http://www.us-cert.gov/cas/techalerts/TA04-196A.html>>

---

Copyright 2004 Carnegie Mellon University.

Terms of use: <<http://www.us-cert.gov/legal.html>>

Revision History

July 14, 2004: Initial release

Last updated July 14, 2004

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.1 (GNU/Linux)

iD8DBQFA9ZD4XlvNRxAkFWARApJoAJ9kLfHwh9rjM39LkWpRYYkPDngD+QCcDj6Q

P8VLUzmOQoMFj+903rIsKHU=

=4I7x

-----END PGP SIGNATURE-----