

# [NT] Vulnerability in Compressed (zipped) Folders Allows Remote Code Execution (MS04-034)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0037.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 10/13/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 13 Oct 2004 15:36:09 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----  
Vulnerability in Compressed (zipped) Folders Allows Remote Code Execution  
(MS04-034)  
-----

## SUMMARY

A remote code execution vulnerability exists in Compressed (zipped) Folders because of an unchecked buffer in the way that it handles specially crafted compressed files. An attacker could exploit the vulnerability by constructing a malicious compressed file that could potentially allow remote code execution if a user visited a malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, user interaction is required to exploit this vulnerability.

Note: Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

## DETAILS

Vulnerable Systems:

\* Microsoft Windows XP and Microsoft Windows XP Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=6B70BA00-56D1-4314-8F53-F8355A6861D3>>

## Securiteam: [NT] Vulnerability in Compressed (zipped) Folders Allows Remote Code Execution (MS04-034)

Download the update

\* Microsoft Windows XP 64-Bit Edition Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3F6896F3-F055-438D-93CE-CD15F37264CB>>

Download the update

\* Microsoft Windows XP 64-Bit Edition Version 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=4B63EF24-D0E4-4005-8E23-2F5EC24BE63F>>

Download the update

\* Microsoft Windows Server 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0903569E-7F3D-4846-A1DC-78734E77D3A9>>

Download the update

\* Microsoft Windows Server 2003 64-Bit Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=4B63EF24-D0E4-4005-8E23-2F5EC24BE63F>>

Download the update

Immune Systems:

\* 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 3 and Microsoft Windows 2000 Service Pack 4

\* Microsoft Windows XP Service Pack 2

\* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (Me)

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0575>>  
CAN-2004-0575

Mitigating Factors for Compressed (zipped) Folders Vulnerability

\* In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site.

\* An attacker who successfully exploited this vulnerability could gain the same privileges as the user. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges.

\* By default, Outlook Express 6, Outlook 2002, and Outlook 2003 open HTML e-mail messages in the Restricted sites zone. Additionally, Outlook 98 and Outlook 2000 open HTML e-mail messages in the Restricted sites zone if the <<http://go.microsoft.com/fwlink/?LinkId=33334>> Outlook E-mail Security Update has been installed. Outlook Express 5.5 Service Pack 2 opens HTML e-mail in the Restricted sites zone if Microsoft Security Bulletin <<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04-018 has been installed. The Restricted sites zone helps reduce attacks that could attempt to exploit this vulnerability.

The risk of attack from the HTML e-mail vector can be significantly reduced if you meet all the following conditions:

\* Apply the update that is included with Microsoft Security Bulletin

## Securiteam: [NT] Vulnerability in Compressed (zipped) Folders Allows Remote Code Execution (MS04–034)

<<http://go.microsoft.com/fwlink?linkid=19873>> MS03–040 or a later Cumulative Security Update for Internet Explorer.

- \* Use Internet Explorer 6 or later.

- \* Use the Microsoft Outlook E–mail Security Update, use Microsoft Outlook Express 6 or later, or use Microsoft Outlook 2000 Service Pack 2 or later in its default configuration.

### Workarounds for Compressed (zipped) Folders Vulnerability

- \* Install <<http://go.microsoft.com/fwlink/?LinkId=33334>> Outlook E–mail Security Update if you are using Outlook 2000 SP1 or earlier, to help protect yourself from the HTML e–mail attack vector.

By default, Outlook Express 6, Outlook 2002 and Outlook 2003 open HTML e–mail messages in the Restricted sites zone. Additionally, Outlook 98 and Outlook 2000 open HTML e–mail messages in the Restricted sites zone if the <<http://go.microsoft.com/fwlink/?LinkId=33334>> Outlook E–mail Security Update has been installed. Outlook Express 5.5 Service Pack 2 opens HTML e–mail in the Restricted sites zone if Microsoft Security Bulletin <<http://go.microsoft.com/fwlink/?LinkId=19527>> MS04–018 has been installed. The Restricted sites zone helps reduce attacks that could attempt to exploit this vulnerability.

- \* Read e–mail messages in plain text format if you are using Outlook 2002 or later, or Outlook Express 6 SP1 or later, to help protect yourself from the HTML e–mail attack vector.

Microsoft Outlook 2002 users who have applied Office XP Service Pack 1 or later and Microsoft Outlook Express 6 users who have applied Internet Explorer 6 Service Pack 1 can enable this setting and view e–mail messages that are not digitally signed or e–mail messages that are not encrypted in plain text only.

Digitally signed e–mail messages or encrypted e–mail messages are not affected by the setting and may be read in their original formats. For more information about enabling this setting in Outlook 2002, see Microsoft Knowledge Base Article

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:307594>> 307594.

For information about this setting in Outlook Express 6, see Microsoft Knowledge Base Article <<http://support.microsoft.com/?kbid=291387>> 291387.

Impact of Workaround: E–mail messages that are viewed in plain text format will not contain pictures, specialized fonts, animations, or other rich content. In addition:

- \* The changes are applied to the preview pane and to open messages.
- \* Pictures become attachments so that they are not lost.
- \* Because the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly.

- \* Do not open or save .zip files that you receive from untrusted sources. This vulnerability could be exploited when a user views a .zip file. Do not open files that use this file name extension if the files are from



## Securiteam: [NT] Vulnerability in Compressed (zipped) Folders Allows Remote Code Execution (MS04-034)

An attacker could also access the affected component through another vector. For example, an attacker could log on to the system interactively or by using another program that passes parameters to the vulnerable component (locally or remotely).

What systems are primarily at risk from the vulnerability ?

Workstations and terminal servers are primarily at risk. Servers are only at risk if users who do not have sufficient administrative credentials are given the ability to log on to servers and to run programs. However, best practices strongly discourage allowing this.

Could the vulnerability be exploited over the Internet ?

Yes. An attacker may be able to exploit this vulnerability over the Internet.

What does the update do ?

The update removes the vulnerability by modifying the way that Compressed (zipped) Folders validates the length of a message before it passes the message to the allocated buffer.

When this security bulletin was issued, had this vulnerability been publicly disclosed ?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information indicating that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited ?

No. Microsoft had not received any information indicating that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

### ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<http://www.microsoft.com/technet/security/bulletin/MS04-034.msp>>

<http://www.microsoft.com/technet/security/bulletin/MS04-034.msp>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

Securiteam: [NT] Vulnerability in Compressed (zipped) Folders Allows Remote Code Execution (MS04-034)

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.