

# [NT] Vulnerability in TNEF Decoding in Microsoft Outlook and Microsoft Exchange Allow Code Execution (MS06-003)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00039.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 15 Jan 2006 19:20:39 +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 TNEF Decoding in Microsoft Outlook and Microsoft Exchange Allow Code Execution (MS06-003)

---

## SUMMARY

A remote code execution vulnerability exists in Microsoft Outlook and Microsoft Exchange Server because of the way that it decodes the Transport Neutral Encapsulation Format (TNEF) MIME attachment.

An attacker could exploit the vulnerability by constructing a specially crafted TNEF message that could potentially allow remote code execution when a user opens or previews a malicious e-mail message or when the Microsoft Exchange Server Information Store processes the specially crafted message. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

## DETAILS

Vulnerable Systems:

- \* Microsoft Office 2000 Service Pack 3
- \* Microsoft Office 2000 Software:

[NT] Vulnerability in TNEF Decoding in Microsoft Outlook and Microsoft Exchange Allow Code Execution (MS06-003)

\* Microsoft Outlook 2000

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=64D0336D-F962-4AB1-A724-9F6BA2108CB9>>

Download the update (KB892842)

\* Microsoft Office 2000 MultiLanguage Packs

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=2C0FA7C7-91AA-49B4-9731-9E83E3E0823D>>

Download the update (KB892842)

\* Microsoft Outlook 2000 English MultiLanguage Packs

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=2C0FA7C7-91AA-49B4-9731-9E83E3E0823D>>

Download the update (KB892842)

\* Microsoft Office XP Service Pack 3

Microsoft Office XP Software:

\* Microsoft Outlook 2002

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9A85CEBB-0D9A-465D-A4BC-AF501562772D>>

Download the update (KB892841)

\* Microsoft Office XP Multilingual User Interface Packs

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=CCA9399A-6DA3-4163-8398-C58DC328182B>>

Download the update (KB892841)

Note Multilingual User Interface Packs are for non-English packages.

\* Microsoft Office 2003 Service Pack 1 and Service Pack 2

Microsoft Office 2003 Software:

\* Microsoft Outlook 2003

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1D156043-B041-4305-8442-3C4E3B832788>>

Download the update (KB892843)

\* Microsoft Office 2003 Multilingual User Interface Packs

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=D69554AD-196F-4789-91E5-B2A753EED854>>

Download the update (KB892843)

\* Microsoft Office 2003 Language Interface Packs

<<http://www.microsoft.com/downloads/details.aspx?FamilyID=db080de8-8193-4c32-9019-9980ecd6874a>>

Download the update (KB887617)

Note Multilingual User Interface Packs are for non-English packages

Microsoft Exchange Server

\* Microsoft Exchange Server 5.0 Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0A8DF1C3-ABF9-4A21-9B49-81FA362B251F>>

Download the update (KB894689)

\* Microsoft Exchange Server 5.5 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=EC6BD30E-12DE-4CA1-9432-D2E73AF62427>>

Download the update (KB894689)

\* Microsoft Exchange 2000 Server Pack 3 with the Exchange 2000

Post-Service Pack 3 Update Rollup of August 2004

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=372FF07F-C3CA-4301-8559-9B90344EDC02>>

Download the update (894689)

Immune Systems:

\* Microsoft Exchange Server 2003 Service Pack 1

\* Microsoft Exchange Server 2003 Service Pack 2

A remote code execution vulnerability exists in Microsoft Outlook and Microsoft Exchange Server because of the way that it decodes the Transport Neutral Encapsulation Format (TNEF) MIME attachment.

An attacker could exploit the vulnerability by constructing a specially crafted TNEF message that could potentially allow remote code execution

[NT] Vulnerability in TNEF Decoding in Microsoft Outlook and Microsoft Exchange Allow Code Execution (M

when a user opens or previews a malicious e-mail message or when the Microsoft Exchange Server Information Store processes the specially crafted message.

An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors for TNEF Decoding Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0002>>  
CVE-2006-0002:

\* Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Workarounds for TNEF Decoding Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0002>>  
CVE-2006-0002:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

\* Block MS-TNEF on Microsoft Exchange Server to help protect against attempts to exploit this vulnerability through SMTP e-mail.

Systems can be configured to block certain types of files from being received as e-mail attachments. Microsoft TNEF-encoded e-mail messages, commonly known as rich text format (RTF) e-mail messages, can contain malicious OLE objects. These e-mail messages contain a file attachment that stores the TNEF information. This file attachment is usually named Winmail.dat. Blocking this file, and blocking the ms-tnef MIME type, could help protect Exchange servers and other affected programs from attempts to exploit this vulnerability if customers cannot install the available security update. To help protect an Exchange Server computer from attacks through SMTP, block the Winmail.dat file and all application/ms-tnef MIME type content before it reaches the Exchange Server computer.

Note You cannot mitigate this vulnerability by setting the Exchange rich-text format option in Exchange Server to Never used or by disabling TNEF processing by editing the registry.

Note Exchange supports other messaging protocols, such as X.400, that these workarounds do not protect. We recommend that administrators require authentication on all other client and message transport protocols to help prevent attacks using these protocols.

Note Filtering only for attachments that have the file name Winmail.dat may not be sufficient to help protect your system. A malicious file attachment could be given another file name that could then be processed by the Exchange Server computer. To help protect against malicious e-mail messages, block all application/ms-tnef MIME type content.

There are many ways to block the Winmail.dat file and other TNEF content.

Here are some suggestions:

\* You can use ISA Server 2000 SMTP Message Screener to block all file attachments or to block only the Winmail.dat file. Blocking all file attachments provides the most protection for this issue if you use ISA Server 2000 because ISA Server 2000 does not support blocking content based on MIME content types. For more information, see <http://support.microsoft.com/?id=315132> Microsoft Knowledge Base Article 315132.

\* You can use ISA Server 2000 SMTP Filter to block all file attachments or to block only the Winmail.dat file. Blocking all file attachments provides the most protection for this issue if you use ISA Server 2000 because ISA Server 2000 does not support blocking content based on MIME content types. For more information, see <http://support.microsoft.com/?id=320703> Microsoft Knowledge Base Article 320703.

\* You can use ISA Server 2004 SMTP Filter and Message Screener block all file attachments or just the Winmail.dat file. Blocking all file attachments provides the most protection for this issue if you use ISA Server 2004 because ISA Server 2004 does not support blocking content based on MIME content types. For more information, see <http://support.microsoft.com/?id=888709> Microsoft Knowledge Base Article 888709.

\* You can use third-party e-mail filters to block all application/ms-tnef MIME type content before it is sent to the Exchange Server computer or to a vulnerable application.

Impact of workaround: If TNEF attachments are blocked, e-mail messages that are formatted as RTF will not be received correctly. In some cases, users could receive blank e-mail messages instead of the original RTF-formatted e-mail message. In other cases, users may not receive e-mail messages that are formatted as RTF at all. Blocking the TNEF attachments will not affect e-mail messages that are formatted as HTML or that are formatted as plain text. Perform this workaround only if you cannot install the available security update or if a security update is not publicly available for your configuration.

\* Require authentication for connections to a server that is running Microsoft Exchange Server for all client and message transport protocols. Requiring authentication for all connections made to the Exchange Server computer will help protect against anonymous attacks. This will not protect against an attack from a malicious user who can successfully authenticate.

Impact of workaround: Anonymous communication from clients through IMAP, POP3, HTTP, LDAP, SMTP, and NNTP will no longer be possible. Server to server anonymous communication through RPC, X.400, foreign gateway, and third-party connector protocols will also no longer be possible. In most

configurations of Exchange Server, authenticated access is already required for all protocols except SMTP. If all application/ms-tnef MIME type message parts and the Winmail.dat file are blocked, as described in the previous workaround, anonymous SMTP connections could still be accepted.

\* Do not accept incoming public newsfeeds through the NNTP protocol on Microsoft Exchange Server.

Incoming newsfeeds are not enabled by default for Exchange Server. If you have subscribed to incoming newsfeeds from public newsgroups, an attacker could post a malicious message to such a newsgroup. Even if you require authentication between the news server and your Exchange Server computer, such a message could still be transferred to your Exchange Server computer. Therefore, you should disable incoming newsfeeds from any NNTP server that could let a user post a malicious message.

Impact of workaround: Exchange access to public newsgroup feeds will no longer be possible.

FAQ for TNEF Decoding Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0002>>  
CVE-2006-0002:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. 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. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

What causes the vulnerability?

Microsoft Exchange Server and Outlook both use the TNEF protocol. The vulnerability lies in the fact that Outlook or Exchange decodes a specially formed e-mail message that uses the TNEF protocol.

What is TNEF?

Transport Neutral Encapsulation (TNEF) is a format used by the Microsoft Exchange Server and Outlook e-mail clients when sending messages formatted as Rich Text Format (RTF). When Microsoft Exchange thinks that it is sending a message to another Microsoft e-mail client, it extracts all the formatting information and encodes it in a special TNEF block. It then sends the message in two parts – the text message with the formatting removed and the formatting instructions in the TNEF block. On the receiving side, a Microsoft e-mail client processes the TNEF block and re-formats the message

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system.

Who could exploit the vulnerability?

Any anonymous user who could deliver a specially crafted message to a user who is running Outlook or Exchange Server could try to exploit this vulnerability.

What systems are primarily at risk from the vulnerability?

Workstations and Microsoft Exchange servers are primarily at risk. Servers could be at more risk if users who do not have sufficient administrative permissions are given the ability to log on to servers and to run programs. However, best practices strongly discourage allowing this.

What does the update do?

The update removes the vulnerability by modifying the way that Outlook and Microsoft Exchange Server validate 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 to indicate 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 to indicate 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 Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS06-003.msp>>

<http://www.microsoft.com/technet/security/Bulletin/MS06-003.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@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====  
=====

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.

- 
- Prev by Date: [\*\[REVS\] Malware – Future Trends\*](#)
  - Next by Date: [\*\[NT\] Windows Embedded Open Type \(EOT\) Font Heap Overflow\*](#)
  - Previous by thread: [\*\[REVS\] Malware – Future Trends\*](#)
  - Next by thread: [\*\[NT\] Windows Embedded Open Type \(EOT\) Font Heap Overflow\*](#)
  - Index(es):
    - ◆ [\*Date\*](#)
    - ◆ [\*Thread\*](#)