

[NT] Mozilla Thunderbird Attachment Spoofing Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00068.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 19 Jan 2006 17:02:34 +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>

Mozilla Thunderbird Attachment Spoofing Vulnerability

SUMMARY

Mozilla Thunderbird displays display attachments in a wrongful manner which allows attackers to spoof attachments and convince users to execute arbitrary programs.

DETAILS

Vulnerable Systems:

- * Mozilla Thunderbird version 1.0.2
- * Mozilla Thunderbird version 1.0.6
- * Mozilla Thunderbird version 1.0.7

Immune Systems:

- * Mozilla Thunderbird version 1.5

The vulnerability is caused due to attachments not being displayed correctly in mails. This can be exploited to spoof the file extension and the associated file type icon via a combination of overly long filenames containing whitespaces and "Content-Type" headers not matching the file extension.

[NT] Mozilla Thunderbird Attachment Spoofing Vulnerability

Successful exploitation may lead to malware being saved to e.g. the desktop.

NOTE: Attachments can be saved by dragging the attachment, or using the "Save As..." or "Save All..." functionality. For files on the desktop the icon can be spoofed if it e.g. is a ".exe" or ".lnk" file.

Disclosure Timeline:

01/07/2005 – Initial vendor notification.
10/07/2005 – Vendor confirms the vulnerability.
27/07/2005 – Vulnerability fixed in the CVS repository.
12/01/2006 – Thunderbird 1.5 released.
17/01/2006 – Public disclosure.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:vuln@xxxxxxxxxxxx>> Secunia Research.

The original article can be found at:

<http://secunia.com/secunia_research/2005-22/advisory/>
http://secunia.com/secunia_research/2005-22/advisory/

The bug report can be found at:

<https://bugzilla.mozilla.org/show_bug.cgi?id=300246>
https://bugzilla.mozilla.org/show_bug.cgi?id=300246

=====

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@xxxxxxxxxxxx

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

=====

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: [\[NT\] EMC Legato Networker DoS and Multiple Buffer Overflows](#)
 - Next by Date: [\[NT\] Internet Explorer XML and IMG Elements DoS](#)
 - Previous by thread: [\[NT\] EMC Legato Networker DoS and Multiple Buffer Overflows](#)

[NT] Mozilla Thunderbird Attachment Spoofing Vulnerability

- Next by thread: [***\[NT\] Internet Explorer XML and IMG Elements DoS***](#)
- Index(es):
 - ◆ [***Date***](#)
 - ◆ [***Thread***](#)