

# [NT] Microsoft Office Buffer Overflow in Routing Slip Metadata (MS06-012)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-03/msg00078.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 23 Mar 2006 14:28:21 +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>

-----

Microsoft Office Buffer Overflow in Routing Slip Metadata (MS06-012)

---

## SUMMARY

There exists a buffer overflow in Microsoft Word, Excel, PowerPoint, and Outlook in the parsing of the routing slip metadata.

The result is that when a user closes a malicious document, arbitrary code can be executed on the host in question.

## DETAILS

Microsoft Office supports the concept of routing slips. These can be embedded within documents to ease the process of collaborative working. It was discovered that within the metadata of Microsoft's document format that there is both a length value and a null terminated string for the different sections of a routing slip. Upon further investigation it was discovered that the affected applications allocate memory based on the size contained within the length field, but then proceeds to copy the entire string up until the null termination.

The result in the case of Microsoft Word 2002 SP3 (fully patched), is that we overwrite the saved return address on the stack with a Unicode value.

[NT] Microsoft Office Buffer Overflow in Routing Slip Metadata (MS06-012)

This can be used to obtain control of the execution within the program.

Microsoft Word, Excel, PowerPoint and Outlook all behave slightly differently and in the case of Office 2003, it appears that the values move from the stack to the heap which makes exploitation more complicated, yet not impossible.

Vendor Response:

The above vulnerability was addressed by  
<<http://www.microsoft.com/technet/security/Bulletin/MS06-012.msp>>  
Microsoft Security Bulletin MS06-012.

Fix:

Apply the patch supplied by Microsoft.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0009>>  
CVE-2006-0009

ADDITIONAL INFORMATION

The information has been provided by Symantec Security Advisory.

The original article can be found at:

<<http://www.securityfocus.com/bid/17000>>  
<http://www.securityfocus.com/bid/17000>

References:

<<http://www.securiteam.com/windowsntfocus/5TP0B1FI0C.html>>  
<http://www.securiteam.com/windowsntfocus/5TP0B1FI0C.html>  
<<http://www.microsoft.com/technet/security/Bulletin/MS06-012.msp>>  
<http://www.microsoft.com/technet/security/Bulletin/MS06-012.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@xxxxxxxxxxxxxxxx

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

=====  
=====

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.