

SYMSA-2006-001: Buffer overflow in Microsoft Office 2000, Office XP (2002), and Office 2003 Routing Slip Metadata

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-03/msg00272.html>

- *From:* CS_Advisories Mailbox <CS_Advisories_Mailbox@xxxxxxxxxxxxx>
 - *Date:* Tue, 14 Mar 2006 11:30:41 -0800
-

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

Hash: SHA1

Symantec Professional Services

www.symantec.com

Security Advisory

Advisory ID : SYMSA-2006-001

Advisory Name: Buffer overflow in Microsoft Office 2000, Office XP (2002), and Office 2003 Routing Slip Metadata.

Release Date : 03-14-2006

Application : Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Outlook

Platform : Windows

Severity : Remotely exploitable / User access

Author : Ollie Whitehouse / ollie_whitehouse@xxxxxxxxxxxxx

Vendor Status: Duplicated and verified by Microsoft, patch available.

CVE Number : CVE-2006-0009

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

Overview:

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. During Symantec's investigation 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. 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 Microsoft Security Bulletin MS06-012. For details see <http://www.microsoft.com/technet/security/Bulletin/MS06-012.msp>

If there are any further questions about this statement, please contact Microsoft support.

Recommendation:

Apply the patch supplied by Microsoft according to your organization's software maintenance test and deployment procedures.

Common Vulnerabilities and Exposures (CVE) Information:

The Common Vulnerabilities and Exposures (CVE) project has assigned the following names to these issues. These are candidates for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

CVE-2006-0009

-----Symantec Consulting Services Advisory Information-----

For questions about this advisory, or to report an error:
cs_advisories@xxxxxxxxxxxx

For details on Symantec's Vulnerability Reporting Policy:

<http://www.symantec.com/research/Symantec-Responsible-Disclosure.pdf>

Consulting Services Advisory Archive:

<http://www.symantec.com/research/>

Consulting Services Advisory PGP Key:

http://www.symantec.com/research/Symantec_Consulting_Services_Advisories_PGP.asc

-----Symantec Product Advisory Information-----

To Report a Security Vulnerability in a Symantec Product:

secure@xxxxxxxxxxxxx

For general information on Symantec's Product Vulnerability reporting and response:

<http://www.symantec.com/security/>

Symantec Product Advisory Archive:

<http://www.symantec.com/avcenter/security/SymantecAdvisories.html>

Symantec Product Advisory PGP Key:

<http://www.symantec.com/security/Symantec-Vulnerability-Management-Key.asc>

Copyright (c) 2006 by Symantec Corp.

Permission to redistribute this alert electronically is granted as long as it is not edited in any way unless authorized by Symantec Consulting Services. Reprinting the whole or part of this alert in any medium other than electronically requires permission from cs_advisories@xxxxxxxxxxxxx

Disclaimer

The information in the advisory is believed to be accurate at the time of publishing based on currently available information. Use of the information constitutes acceptance for use in an AS IS condition. There are no warranties with regard to this information. Neither the author nor the publisher accepts any liability for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this information.

Symantec, Symantec products, and Symantec Consulting Services are registered trademarks of Symantec Corp. and/or affiliated companies in the United States and other countries. All other registered and unregistered trademarks represented in this document are the sole property of their respective companies/owners.

SYMSA-2006-001: Buffer overflow in Microsoft Office 2000, Office XP (2002), and Office 2003 Routing Slip Metadata

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

Version: PGP 8.1

iQA/AwUBRBcZsnvrrLpIdMO6EQIMiQCg3Xc9RH0tk3zhThEvLanxhhvj2tIAoMuW

55u11JffbKu3mqOOlrcxhBO/

=elwo

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