

[NT] Microsoft Word 6.0/95 Document Converter Buffer Overflow (MS04-041)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0033.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/15/04

To: list@securiteam.com

Date: 15 Dec 2004 19:26:31 +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 Word 6.0/95 Document Converter Buffer Overflow (MS04-041)

SUMMARY

WordPad is "a word processing application that uses the MFC rich edit control classes. It is installed by default on most Windows platforms, and contains filters for converting from other filetypes into RTF (Rich Text Format)".

Remote exploitation of a buffer overflow vulnerability in Microsoft Corp.'s Word 6.0/95 Document Converter could allow attackers to exploit arbitrary code under the privileges of the target user.

DETAILS

The Microsoft Word 6.0/95 Document Converter (MSWRD632.WPC) is a module that is utilized by WordPad and potentially other applications to convert Microsoft Word format files into the Rich Text Format natively handled by WordPad. The module is installed by default in:

C:\Program Files\Common Files\Microsoft Shared\TextConv

The problem specifically exists when a specially crafted file is opened by

Securiteam: [NT] Microsoft Word 6.0/95 Document Converter Buffer Overflow (MS04-041)

WordPad or another application that utilizes the vulnerable library and results in a buffer overflow. The overflow is caused by copying a length tagged segment of a file into a fixed length stack buffer of smaller size. The following instruction sequence is found within ConvertForeignToRtf():

```
0150eba6 8bd1 mov edx, ecx
0150eba8 83e203 and edx, 0x3
0150ebab c1e902 shr ecx, 0x2
0150ebae f3a5 rep movsd edi, esi
```

This instruction sequence will copy bytes from the memory region pointed to by ESI into the memory region pointed to by EDI. Due to a lack of bounds checking, an overflow occurs directly overwriting the stored return address and frame pointer on the stack and allowing for the eventual execution of arbitrary code.

Analysis:

Successful exploitation allows remote attackers to execute arbitrary code under the privileges of the target user that opened the malicious document. WordPad, a vulnerable application, is installed by default and will open WRI and large TXT files. If Microsoft Word is not installed, WordPad will also be the default application for opening DOC and RTF files.

In order for this vulnerability to be exploited, a user would need to open an attacker-supplied file with a vulnerable application.

Detection:

The following operating systems appear to be impacted by this vulnerability in their default configuration:

- Windows XP
- Windows 2000
- Windows 2003
- Windows NT 4.0
- Windows ME
- Windows 98

iDEFENSE Labs has confirmed that MSWRD632.WPC, file version 1999.8.7.0 is vulnerable. Any application that utilizes this module to convert Word documents may be considered vulnerable. This includes wordpad.exe, which is the default application for opening files with the .wri extension, and doc and .rtf files if Microsoft Word is not installed.

It does not seem to be possible to exploit Microsoft Word itself with this vulnerability, as it does not appear to use this library.

As this module comes with Windows by default, even if you have Word installed, WordPad is still vulnerable to exploitation from files with the .wri extension, or by opening an affected file from within WordPad.

Securiteam: [NT] Microsoft Word 6.0/95 Document Converter Buffer Overflow (MS04-041)

Workaround:

User awareness is the best defense against this class of attack. Users should be aware of the existence of such attacks and proceed with caution when following links or opening attachments from suspicious and/or unsolicited e-mail.

Alternatively, concerned users can remove the affected converter module, MSWRD632.WPC. This will prevent the user from opening Word for Windows files, but will still allow other supported file types to be opened such as .txt or .rtf. However, the error will be handled gracefully and the described vulnerability will no longer be exploitable.

Vendor Response:

This vulnerability is addressed in Microsoft Security Bulletin MS04-041 available at:

<http://www.microsoft.com/technet/security/Bulletin/MS04-041.msp>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0901>>
CAN-2004-0901

Disclosure Timeline:

09/22/2004 – Initial vendor notification
09/23/2004 – Initial vendor response
12/14/2004 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:idlabs-advisories@idefense.com>> iDEFENSE.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=162&type=vulnerabilities>>
<http://www.idefense.com/application/poi/display?id=162&type=vulnerabilities>

=====

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

=====

=====

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.