

[NT] Additional Information Released on Microsoft WordPerfect Document Converter Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0013.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/07/03

To: list@securiteam.com

Date: 7 Sep 2003 10:42:47 +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>

Additional Information Released on Microsoft WordPerfect Document Converter Buffer Overflow

SUMMARY

The Microsoft Word "WordPerfect" document converter included in Microsoft Word has a buffer overflow bug. If the WordPerfect document converter is installed, (by default it is in Office 2000), and a malicious .doc file is opened, there exists the ability for an attacker to execute arbitrary code.

This buffer overflow bug can also happen within Internet Explorer, because Microsoft Word is executed automatically as a helper-application when a doc file is received.

This buffer overflow overwrites the return address in the stack area. We confirmed that arbitrary code could be executed by using this buffer overflow bug.

DETAILS

Systems Affected:

* Microsoft Office 97, 2000, XP

Securiteam: [NT] Additional Information Released on Microsoft WordPerfect Document Converter Buffer Overflow

- * Microsoft Word 98 (J)
- * Microsoft FrontPage 2000, 2002
- * Microsoft Publisher 2000, 2002
- * Microsoft Works Suite 2001, 2002, 2003

While parsing a WordPerfect file, the WordPerfect converter copies data stored in the .doc file to a local buffer. If we modify some bytes of the doc file, we can specify the data offset and data size. The WordPerfect converter does not properly check the size of the data contained in the doc file, and tries to copy all of the data from the file to the local buffer allocated in the stack area. This results in a typical buffer overflow vulnerability in which we can set any value for EIP.

The process for making the .doc file to confirm this buffer overflow is as follows:

[Technical data may wrap in e-mail, please visit
<<http://www.eeye.com/html/Research/Advisories/AD20030903-1.html>>
<http://www.eeye.com/html/Research/Advisories/AD20030903-1.html>.]

1. Open Word and save an empty document as WordPerfect 5.0 file. 2. Open the .doc file in a binary editor. You will be able to confirm the following dump image:

ADDRESS 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0123456789ABCDEF

```
--
00000000 FF 57 50 43 6D 02 00 00 01 0A 00 00 00 00 00 00 .WPCm.....
...
00000130 00 00 00 00 CD 01 00 00 08 00 02 00 00 00 CD 01 .....
...
000001C0 61 75 74 68 6F 72 00 65 45 79 65 00 00 00 00 FB author.eEye....
000001D0 FF 05 00 32 00 00 00 00 00 01 01 6C 00 00 00 01 ...2.....1....
000001E0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

3. Modify 0x00 to 0x01 in offset 0x00000139.
4. Modify 0x00 to the value more than 0x80 in offset 0x000001D8. 5. Modify 0x00 to the value more than 0x01 in offset 0x000001E1 to 0x000001FF. 6. Append garbage data (e.g., a long string of A's) onto the end of this file.

Vendor Status:

Microsoft was notified on May 6, 2003, and has released a patch for this vulnerability. The patch is available at:

<<http://www.securiteam.com/windowsntfocus/5MP0415B5S.html>>

<http://www.microsoft.com/technet/security/bulletin/MS03-036.asp>.

ADDITIONAL INFORMATION

The information has been provided by <mailto:marc@eeye.com> Marc Maiffret of eEye.

=====

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@

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

=====

=====

DISCLAIMER:

Securiteam: [NT] Additional Information Released on Microsoft WordPerfect Document Converter Buffer Overflow

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,