

[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>