



October 10, 2006

McAfee, Inc.
McAfee Avert™ Labs Security Advisory
Public Release Date: 2006-10-10

MS06-060: Microsoft Word Memmove Code Execution Vulnerability

CVE-2006-3647

- **Synopsis**

An integer bug (stack overflow) exists in the Microsoft Word file format. The file format allows a attacker to create a malicious Microsoft Word document that when opened, will execute arbitrary code.

- **Vulnerable Systems**

Microsoft Word 2000
Microsoft Word 2002
Microsoft Word 2003
Microsoft Word 2004 for Mac
Microsoft Word v. X for Mac

- **Vulnerability Information**

CVE-2006-3647

The specific flaw exists during the processing of a malicious WordDocument file. The overflow can be triggered during the parsing at offset 0xb4c in the WordDocument stream. At this offset, there is a WORD size that is used as the third parameter to a memmove call. If the size passed to memmove is > 0x8000, it will extend to DWORD(0x8000 = 0xffff8001), and will copy 0xffff8001 bytes to the stack.

This is a code execution vulnerability that may be exploited to compromise users that open a malformed Microsoft Word document.

- **Resolution**

Install the Microsoft-provided vendor patch.

Further information is available at: <http://www.microsoft.com/technet/security/Bulletin/MS06-060.msp>

- **Credits**

This vulnerability was discovered by Chen Xiao Bo of McAfee Avert Labs.

- **Legal Notice**

Copyright (C) 2006 McAfee, Inc.

The information contained within this advisory is provided for the convenience of McAfee's customers, and may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way. McAfee makes no representations or warranties regarding the accuracy of the information referenced in this document, or the suitability of that information for your purposes.

McAfee, Inc. and McAfee Avert Labs are registered Trademarks of McAfee, Inc. and/or its affiliated companies in the United States and/or other Countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.