



August 14, 2007

McAfee, Inc.
McAfee® Avert® Labs Security Advisory
Public Release Date: 2007-08-14

Virtual PC and Virtual Server Heap Overflow Vulnerability

CVE-2007-0948

- **Synopsis**

A heap overflow vulnerability exists in MS Virtual PC and MS Virtual Server that allows a guest OS user to execute arbitrary code on the host.

- **Vulnerable System or Application**

Microsoft Virtual PC 2004
Microsoft Virtual PC 2004 Service Pack 1
Microsoft Virtual Server 2005 Standard Edition
Microsoft Virtual Server 2005 Enterprise Edition
Microsoft Virtual Server 2005 R2 Standard Edition
Microsoft Virtual Server 2005 R2 Enterprise Edition
Microsoft Virtual PC for Mac Version 6.1
Microsoft Virtual PC for Mac Version 7

- **Vulnerability Information**

A guest OS running under the control of Virtual PC or Virtual Server can exchange messages with the virtual machine monitor via dedicated assembly instructions. When parsing a certain type of such messages, the virtual machine monitor does not sanitize all fields in the message, which may lead to a heap overflow within the VMM and execution of arbitrary code on the host.

- **Resolution**

Microsoft has released a security bulletin and associated patch for this vulnerability:
<http://www.microsoft.com/technet/security/Bulletin/MS07-049.msp>

- **Credits**

This vulnerability was discovered by Rafal Wojtczuk of McAfee Avert Labs.

- **Legal Notice**

Copyright (C) 2007 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.