



September 20, 2007

McAfee, Inc.
McAfee® Avert® Labs Security Advisory
Public Release Date: 2007-09-20

Memory Corruption in VMWare VM emulators

CVE-2007-4497

- **Synopsis**

Multiple vulnerabilities exist in VMware VM emulators; the most severe one can potentially allow a guest OS user to execute arbitrary code on the host.

- **Vulnerable System or Application**

VMware Workstation 6.0.0
VMware Workstation 5.5.4
VMware Player 2.0.0
VMware Player 1.0.4
VMware Server 1.0.3
VMware ACE 2.0.0
VMware ACE 1.0.3

- **Vulnerability Information**

CVE-2007-4496

A guest OS running under the control of the affected VMware products can exchange messages with the virtual machine monitor by accessing the I/O port number 0x5658. When parsing a certain type of such messages, the virtual machine monitor does not sanitize all fields in the message. In default configuration, it is possible to force the VMM to read from an invalid memory location or enter infinite loop. In non-default configuration, it is possible to force the VMM to write past the end of a heap buffer, which may lead to execution of arbitrary code on the host.

- **Resolution**

VMware has released a security bulletin VMSA-2007-0006 and associated patch for these vulnerabilities.

- **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.