



March 17, 2008

McAfee, Inc.
McAfee® Avert® Labs Security Advisory
Public Release Date: 2008-03-17

VMware VMX Local Privilege Escalation

CVE-2008-1363

- **Synopsis**

Local Privilege Escalation on Windows based platforms by Hijacking VMware VMX configuration file

- **Vulnerable System or Application**

VMware Workstation 6.0 upgrade to version 6.0.3 (Build# 80004)
VMware Workstation 5.5 upgrade to version 5.5.6 (Build# 80404)
VMware Player 2.0 upgrade to version 2.0.3 (Build# 80004)
VMware Player 1.0 upgrade to version 1.0.6 (Build# 80404)
VMware Server 1.0 upgrade to version 1.0.5 (Build# 80187)
VMware ACE 2.0 upgrade to version 2.0.1 (Build# 80004)
VMware ACE 1.0 upgrade to version 1.0.5 (Build# 79846)

- **Vulnerability Information**

CVE-2008-1363

VMware Workstation 6.0.x before 6.0.3 and 5.5.x before 5.5.6, VMware Player 2.0.x before 2.0.3 and 1.0.x before 1.0.6, VMware ACE 2.0.x before 2.0.1 and 1.0.x before 1.0.5, and VMware Server 1.0.x before 1.0.5 on Windows allow local users to gain privileges via an unspecified manipulation of a config.ini file located in an Application Data folder, which can be used for "hijacking the VMX process."

- **Resolution**

Patches were provided by vendor VMware. (<http://www.vmware.com/security/advisories/VMSA-2008-0005.html>)

- **Credits**

This vulnerability was discovered by Sun Bing 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.