



December 9, 2008

---

McAfee, Inc.  
McAfee® Avert® Labs Security Advisory  
Public Release Date: 2008-12-09

Windows Common AVI Parsing Overflow Vulnerability

CVE-2008-4255

---

- **Synopsis**

A vulnerability exists in a Windows Common ActiveX control which may allow remote attackers to execute arbitrary code.

---

- **Vulnerable System or Application**

Microsoft Visual Basic 6.0  
Visual Studio .NET 2002 SP1  
Visual Studio .NET 2003 SP1  
Visual Fox Pro 8.0 SP1  
Visual Fox Pro 9.0 SP1/SP2  
Office Project 2003 SP3  
Office Project 2007 Gold

---

- **Vulnerability Information**

CVE-2008-4255

An AVI file with a specially crafted length may cause an allocation error which resulting in memory corruption which can allow an attacker to execute arbitrary code.

---

- **Resolution**

Microsoft has released a security bulletin MS08-070 and associated patch for this vulnerability.

---

- **Credits**

This vulnerability was discovered by Mark Dowd 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.