



September 12, 2006

---

McAfee, Inc.  
McAfee Avert™ Labs Security Advisory  
Public Release Date: 2006-09-12

### Apple QuickTime Multiple Vulnerabilities

CVE-2006-4382, CVE-2006-4384, CVE-2006-4385, CVE-2006-4386, CVE-2006-4388,  
CVE-2006-4389

---

- **Synopsis**

Apple QuickTime is a multimedia technology used to process image, audio and video data. QuickTime is used by the Mac OS X operating system and by the QuickTime media player for Microsoft Windows.

Seven code execution vulnerabilities are present in QuickTime support for various multimedia formats including: MOV, H.264, FLC, FPX and SGI.

Exploitation could lead to execution of arbitrary code. User interaction is required for an attack to succeed.

The risk rating for these issues is medium.

---

- **Vulnerable Systems**

QuickTime 7.1.2 and below for Mac OS X  
QuickTime for Windows 7.1.2 and below

---

- **Vulnerability Information**

CVE-2006-4382

Two buffer overflow vulnerabilities are present in QuickTime MOV format support.

CVE-2006-4384

On heap overflow vulnerability is present in QuickTime FLC format support.

CVE-2006-4385

One buffer overflow vulnerability is present in QuickTime SGI format support.

CVE-2006-4386

One buffer overflow vulnerability is present in QuickTime MOV H.264 format support.

CVE-2006-4388

One buffer overflow vulnerability is present in QuickTime FlashPix (FPX) format support.

CVE-2006-4389

One uninitialized memory access vulnerability is present in QuickTime FlashPix (FPX) format support.

---

- **Resolution**

Apple has included fixes for the QuickTime issues in QuickTime version 7.1.3 for Mac OS X and for Microsoft Windows.

Further information is available at: <http://docs.info.apple.com/article.html?artnum=304357>

---

- **Credits**

These vulnerabilities were discovered by Mike Price 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.