

# US-CERT Technical Cyber Security Alert TA08-016A -- Apple QuickTime Updates for Multiple Vulnerabilities

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Cert/2008-01/msg00001.html>

---

- *From:* CERT Advisory <[cert-advisory@xxxxxxxx](mailto:cert-advisory@xxxxxxxx)>
  - *Date:* Wed, 16 Jan 2008 15:39:23 -0500
- 

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

National Cyber Alert System

Technical Cyber Security Alert TA08-016A

Apple QuickTime Updates for Multiple Vulnerabilities

Original release date: January 16, 2008

Last revised: --

Source: US-CERT

Systems Affected

- \* Apple Mac OS X running versions of QuickTime prior to 7.4
- \* Microsoft Windows running versions of QuickTime prior to 7.4

Overview

Apple QuickTime contains multiple vulnerabilities. Exploitation of these vulnerabilities could allow a remote attacker to execute arbitrary code or cause a denial-of-service condition.

## I. Description

Apple QuickTime 7.4 resolves multiple vulnerabilities in the way different types of image and media files are handled. An attacker could exploit these vulnerabilities by convincing a user to access a specially crafted image or media file that could be hosted on a web page.

Note that Apple iTunes installs QuickTime, so any system with iTunes

is vulnerable.

## II. Impact

These vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial-of-service condition. For further information, please see About the security content of QuickTime 7.4.

## III. Solution

### Upgrade QuickTime

Upgrade to QuickTime 7.4. This and other updates for Mac OS X are available via Apple Update.

### Secure your web browser

To help mitigate these and other vulnerabilities that can be exploited via a web browser, refer to Securing Your Web Browser.

## References

\* About the security content of the QuickTime 7.4 Update –  
<<http://docs.info.apple.com/article.html?artnum=307301>>

\* How to tell if Software Update for Windows is working correctly when no updates are available –  
<<http://docs.info.apple.com/article.html?artnum=304263>>

\* Apple – QuickTime – Download –  
<<http://www.apple.com/quicktime/download/>>

\* Mac OS X: Updating your software –  
<<http://docs.info.apple.com/article.html?artnum=106704>>

\* Securing Your Web Browser –  
<[http://www.us-cert.gov/reading\\_room/securing\\_browser/](http://www.us-cert.gov/reading_room/securing_browser/)>

---

The most recent version of this document can be found at:

<<http://www.us-cert.gov/cas/techalerts/TA08-016A.html>>

---

Feedback can be directed to US-CERT Technical Staff. Please send email to <cert@xxxxxxxx> with "TA08-016A Feedback VU#818697" in the

subject.

---

For instructions on subscribing to or unsubscribing from this mailing list, visit <<http://www.us-cert.gov/cas/signup.html>>.

---

Produced 2007 by US-CERT, a government organization.

Terms of use:

<<http://www.us-cert.gov/legal.html>>

---

#### Revision History

January 16, 2007: Initial release

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.1 (GNU/Linux)

```
iQEVAwUBR45mevRFkHkM87XOAQLP6AgAj7J4sy83ZWEKfcDb2brgHptxAwqvArkZ
HzV+5lGg1A86V4/MARlxXctWv5JH3e2knx5ZoMUN8napP9VEag2Ra68Zdh9lKu1S
nfCRRwcIj38iakuv7xKrNt1AJHj3rHguzCjvWu8gHEJtlb15zqVr97Ci9LuNdLP3
W4hdsIxuzYQl7Ou5+j0Z9bhH1WWZRjmabsop+b0ApXeZI2F6mJn0rscRvxPQYBlS
ims6CP7YseK4+ElJHAMEJfW/6gPhwyedjgesd0jssYvhtYdufn4OCZvwL+p9QSIQ
+E+UKcws4BHIEpg0dQhA13REQxwqqMgSWdm3NU8hbGdEJAJGH0cYNQ==
=emKJ
```

-----END PGP SIGNATURE-----