

[NT] Apple QuickTime Macintosh Resource Processing Heap Corruption Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-01/msg00034.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 16 Jan 2008 13:53:54 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Apple QuickTime Macintosh Resource Processing Heap Corruption Vulnerability

SUMMARY

<<http://www.apple.com/quicktime/>> QuickTime is "Apple's media player product, and is used to render video and other media". Remote exploitation of a heap corruption vulnerability in Apple Computer Inc.'s QuickTime media player could allow attackers to execute arbitrary code in the context of the targeted user.

DETAILS

Vulnerable Systems:

- * QuickTime Player version 7.3.1

Immune Systems:

- * QuickTime Player version 7.4

The vulnerability specifically exists in the handling of Macintosh Resources embedded in QuickTime movies. When processing these records, a length value stored in the resource header is not properly validated. When a length value larger than the actual buffer size is supplied, potentially

[NT] Apple QuickTime Macintosh Resource Processing Heap Corruption Vulnerability

exploitable memory corruption occurs.

Analysis:

Exploitation of this vulnerability allows attackers to execute arbitrary code in the context of the targeted user. In order to exploit this vulnerability, an attacker must persuade a user into using QuickTime to open a specially crafted QuickTime movie file.

Vendo response:

Apple has released QuickTime 7.4 which resolves this issue. More information is available via Apple's QuickTime Security Update page at the URL: <<http://docs.info.apple.com/article.html?artnum=307301>>
<http://docs.info.apple.com/article.html?artnum=307301>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0032>>
CVE-2008-0032

Disclosure Timeline:

- 09/13/2007 – Initial vendor notification
- 09/13/2007 – Initial vendor response
- 01/15/2008 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense Labs.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=642>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=642>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.