

[NEWS] Multiple Vulnerabilities in Apple QuickTime (Opcode, PICT, Color Table)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-11/msg00016.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 6 Nov 2007 13:44:30 +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>

Multiple Vulnerabilities in Apple QuickTime (Opcode, PICT, Color Table)

SUMMARY

Multiple vulnerabilities have been discovered in Apple's QuickTime player which allows attackers to overflow internal buffers by utilizing vulnerabilities found in the parser of the PICT file format.

DETAILS

Vulnerable Systems:

- * Apple QuickTime version 7.2

Apple QuickTime Uncompressedfile Opcode Stack Overflow Vulnerability

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Apple QuickTime. User interaction is required to exploit this vulnerability in that the target must open a malicious image file.

The specific flaw exists in the parsing of the pict file format. If an invalid length is specified for the UncompressedQuickTimeData opcode, a stack based buffer overflow occurs, allowing the execution of arbitrary code.

[NEWS] Multiple Vulnerabilities in Apple QuickTime (Opcode, PICT, Color Table)

Vendor Response:

Apple has issued an update to correct this vulnerability. More details can be found at: <<http://docs.info.apple.com/article.html?artnum=306896>>
<http://docs.info.apple.com/article.html?artnum=306896>

Disclosure Timeline:

2007.09.14 – Vulnerability reported to vendor
2007.11.05 – Coordinated public release of advisory

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4672>>
CVE-2007-4672

Apple QuickTime PICT File Poly Opcodes Heap Corruption Vulnerability
This vulnerability allows attackers to execute arbitrary code on vulnerable installations of Apple QuickTime. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

The specific flaw exist in the parsing of Poly type opcodes (opcodes 0x0070–74). Due to improper handling of a malformed element in the structure heap corruption occurs. If properly constructed this can lead to code execution.

Vendor Response:

Apple has issued an update to correct this vulnerability. More details can be found at: <<http://docs.info.apple.com/article.html?artnum=306896>>
<http://docs.info.apple.com/article.html?artnum=306896>

Disclosure Timeline:

2007.09.14 – Vulnerability reported to vendor
2007.11.05 – Coordinated public release of advisory

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4676>>
CVE-2007-4676

Apple Quicktime PICT File PackBitsRgn Parsing Heap Corruption Vulnerability

This vulnerability allows attackers to execute arbitrary code on vulnerable installations of Apple QuickTime. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

The specific flaw exist in the parsing of the PackBitsRgn field (Opcode 0x0099). Due to improper handling of a malformed element in the structure, heap corruption occurs. If properly constructed this can lead to code execution running under the credentials of the user.

Vendor Response:

[NEWS] Multiple Vulnerabilities in Apple QuickTime (Opcode, PICT, Color Table)

Apple has issued an update to correct this vulnerability. More details can be found at: <<http://docs.info.apple.com/article.html?artnum=306896>>
<http://docs.info.apple.com/article.html?artnum=306896>

Disclosure Timeline:

2007.09.14 – Vulnerability reported to vendor
2007.11.05 – Coordinated public release of advisory

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4676>>
CVE-2007-4676

Apple QuickTime Color Table RGB Parsing Heap Corruption Vulnerability
This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Apple QuickTime. User interaction is required to exploit this vulnerability in that the target must open a malicious file.

The specific flaw exists in the parsing of the CTAB atom. While reading the CTAB RGB values, an invalid color table size can cause QuickTime to write past the end of the heap chunk. This memory corruption can lead to the execution of arbitrary code.

Vendor Response:

Apple has issued an update to correct this vulnerability. More details can be found at: <<http://docs.info.apple.com/article.html?artnum=306896>>
<http://docs.info.apple.com/article.html?artnum=306896>

Disclosure Timeline:

2007.09.14 – Vulnerability reported to vendor
2007.11.05 – Coordinated public release of advisory

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4677>>
CVE-2007-4677

ADDITIONAL INFORMATION

The information has been provided by <<mailto:zdi-disclosures@xxxxxxxx>>
The Zero Day Initiative (ZDI).

The original article can be found at:

<<http://www.zerodayinitiative.com/advisories/ZDI-07-065.html>>
<http://www.zerodayinitiative.com/advisories/ZDI-07-065.html>,
<<http://www.zerodayinitiative.com/advisories/ZDI-07-066.html>>
<http://www.zerodayinitiative.com/advisories/ZDI-07-066.html>,
<<http://www.zerodayinitiative.com/advisories/ZDI-07-067.html>>
<http://www.zerodayinitiative.com/advisories/ZDI-07-067.html> and
<<http://www.zerodayinitiative.com/advisories/ZDI-07-068.html>>
<http://www.zerodayinitiative.com/advisories/ZDI-07-068.html>

=====

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@xxxxxxxxxxxxxxxxx

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

=====

=====

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.