

# [NEWS] Quartz Composer / QuickTime 7 Information Leakage

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0094.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 05/17/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 17 May 2005 10:55:24 +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>

-----

Quartz Composer / QuickTime 7 Information Leakage

---

## SUMMARY

Quartz Composer files are created with the Quartz Composer application included with the developer tools. The compositions (QTZ files) it creates can be used as screen savers, viewed as they are in the application or embedded as QT atoms in a '.mov' container. As such, they can be viewed in a wide-ranging array of environments, including a web browser, Keynote 2 and the Finder.

Compositions have access to a number of powerful tools (patches), each providing or acting-upon information, ultimately resulting in a graphic composition. The design assumption seems to be that these details should always be contained within the presentation. However, by combining patches that provide advanced system information with patches that load information from the Internet, a malicious '.mov' file (viewed for example by the QuickTime web plugin) can leak this information to an external host.

This issue has not been addressed by Apple yet, and because details of the potential exploit appeared in a public forum shortly after David had notified the vendor, a fix may still be some time away. A temporary

## Securiteam: [NEWS] Quartz Composer / QuickTime 7 Information Leakage

work-around is disabling the QuickTime plugin and treating Quartz Composer files with suspicion.

### DETAILS

#### Vulnerable Systems:

- \* Apple Mac OS X 10.4 (QuickTime 7)

#### Immune Systems:

- \* Apple Mac OS X 10.3.9 (QuickTime 6.5, 7)
- \* QuickTime for Windows

#### Impact:

The information that can be leaked by this method includes (but may not be limited to):

- \* Local user name (long and short)
- \* Computer name
- \* Local IP
- \* OS / kernel version
- \* CPU / RAM / GPU configuration
- \* Names (human-readable) of Bonjour services on the local network
- \* Local or system time
- \* Volume of audio input
- \* Lists of images (including pdfs) matching arbitrary spotlight queries
- \* Lists of images (including pdfs) in specific directories (relative to / or ~)
- \* The existence of image and movie files can indicate the existence of certain software packages

This information can be used for profiling of potential victims, for further use in attacks against the user's system or phishing related social engineering.

#### Proof of Concept:

A proof-of-concept in the form of a Quartz Composer composition embedded in a '.mov' file is available at the following link. Please see that document for more information:

<http://remahl.se/david/vuln/018/demo.html>  
<http://remahl.se/david/vuln/018/demo.html>

#### Technical Details:

The basic attack works as follows:

1. A patch providing the information (for example the Host Info patch) is created (A)
2. The output of (A) is connected to a JavaScript patch which uses `encodeURIComponent()` to URI encode the string (B).
3. The output of (B) is connected to a String Printer which results in a URI, for example (C)
4. The output of (C) is connected to the URL input connection of either the Image Downloader patch or the RSS Feed patch. (D)
5. The output of (D) must be used somehow, otherwise this part of the

Securiteam: [NEWS] Quartz Composer / QuickTime 7 Information Leakage

patch graph will not be used. Rendering the output (via a String to Image) to a 0-sized billboard is fine.

6. When the (D) patch is activated, it will access the URI (output of (C)), thus leaking the restricted information to an HTTP host of the attacker's choice.

Vendor contact:

Apple Computer's security team was contacted with information about the issue on 2005-05-06. Following a discussion of this problem on the public quartzcomposer-dev mailinglist (initiated by a third-party), the full details of the problems were released on May 11.

Vendor response:

Apple Computer - 2005-05-10, 04:50 UTC: Confirmed receipt of problem report(did not confirm issue).

ADDITIONAL INFORMATION

The information has been provided by <mailto:vuln@remahl.se> David Remahl.

The original article can be found at: <<http://remahl.se/david/vuln/018/>>  
<http://remahl.se/david/vuln/018/>

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.