

[Full-disclosure] [DR018] Quartz Composer / QuickTime 7 information leakage

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-05/0281.html>

From: David Remahl (vuln_at_remahl.se)

Date: 05/12/05

To: SecurityTracker <bugs@securitytracker.com>, VulnWatch <vulnwatch@vulnwatch.org>, Secunia <secunia@secunia.com>

Date: Thu, 12 May 2005 02:00:39 +0200

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

Hash: SHA1

The canonical URI of this advisory is <<http://remahl.se/david/vuln/018/>>.

This advisory concerns an as-yet unpatched problem in QuickTime 7 on Mac OS X 10.4. The reason for disclosure before a vendor patch is that another person realized the potential problem independently and posted a message about it to the public mailing list quartzcomposer-dev (hosted by Apple).

The suggested workaround is to disable the QuickTime browser plugin until a fix is available from the vendor.

/ Regards, David Remahl

DR018: Quartz Composer / QuickTime 7 information leakage

=====

Date of discovery: 2005-04-26

Date of publication: 2005-05-11

Discovered by: David Remahl <david@remahl.se>

Advisory URL: <http://remahl.se/david/vuln/018/>

CVEs: n/a [as of this writing, the author is aware of no CVEs assigned to this vulnerability]

Classification: information exposure; design error

License: Public Domain

AFFECTED PRODUCTS

Verified vulnerable:

- * Apple Mac OS X 10.4 (QuickTime 7)

Verified safe:

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

INTRODUCTION

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 envi