

[VulnWatch] Apple QuickTime ActiveX v5.0.2 Buffer Overrun (a091002-1)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-09/0012.html>

From: @stake Advisories (@stake)

Date: 09/10/02

From: "@stake Advisories" <advisories@atstake.com>

To: <vulnwatch@vulnwatch.org>

Date: Tue, 10 Sep 2002 16:53:21 -0400

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

Hash: SHA1

@stake Inc.
www.atstake.com

Security Advisory

Advisory Name: Apple QuickTime ActiveX v5.0.2 Buffer Overrun

Release Date: 09/10/2002

Application: Apple QuickTime ActiveX v5.0.2

Platform: Windows NT4 SP6a, Windows 2000 SP1

Windows XP

Severity: There is a buffer overflow condition that
can result in execution of arbitrary
code.

Author: Ollie Whitehouse [ollie@atstake.com]

Contributions: Andreas Junestam [andreas@atstake.com]

Dave Aitel

Vendor Status: Vendor has fixed software update

CVE Candidate: CAN-2002-0376

Reference: www.atstake.com/research/advisories/2002/a091002-1.txt

Overview:

Apple QuickTime (<http://www.quicktime.com>) is the media player used by a large number of distributors for high quality video and audio based media. Version 5.0 has been downloaded over 100,000,000 times. There is a buffer overrun caused by the way that the QuickTime ActiveX component handles the "pluginspage" field when parsed from a malicious remote or local HTML page. This can allow the execution of arbitrary computer code on the computer viewing the malicious web page. The QuickTime ActiveX component is commonly used for movie trailers (i.e. those located at <http://www.apple.com/trailers/>) and

VulnWatch: [VulnWatch] Apple QuickTime ActiveX v5.0.2 Buffer Overrun (a091002-1)

other streaming or static media technologies when they are embedded in a web page.

Details:

To exploit this vulnerability an attacker would need to get his or her target to open a malicious HTML file as an attachment to an email message, as a file on the local or network file system, or as a file via HTTP. Most likely this would be accomplished by embedding a link to a vulnerable web site in an email message or another web page. If the malicious HTML file is opened it will cause Quicktime to execute the arbitrary computer code contained within the HTML page.

Take the following example HTML page:

```
----- Begin Sample HTML
<OBJECT CLASSID="clsid:02BF25D5-8C17-4B23-BC80-D3488ABDDC6B"
  WIDTH="480" HEIGHT="376">
  <PARAM NAME="src" VALUE="test.mov">
  <PARAM NAME="controller" VALUE="false">
  <PARAM NAME="target" VALUE="myself">
  <PARAM NAME="href" VALUE="test.mov">
  <PARAM NAME="pluginspage" VALUE="insert overly long
string here">
  <EMBED WIDTH="480" HEIGHT="376" CONTROLLER="false"
  TARGET="myself" HREF="test2.mov"
  SRC="test.mov"
  BGCOLOR="FFFFFF"
  BORDER="0"
  PLUGINSAGE="insert overly long string here">
  </EMBED>
</OBJECT>
----- End Sample HTML
```

[note: remove the '7's in the tags above to create valid HTML]

This sample HTML when, edited to insert an overly long string, will cause an exception that is exploitable.

It is possible for an attacker to specify a codebase that will download a vulnerable version of the ActiveX component.

This is a good example of why not to trust *ANY* ActiveX components from any unknown source even if the site is considered safe and the ActiveX component is signed on behalf of a trusted organization.

Vendor Response:

Apple was notified of this issue by @stake on May 13, 2002.

VulnWatch: [VulnWatch] Apple QuickTime ActiveX v5.0.2 Buffer Overrun (a091002-1)

Apple has resolved this issue within QuickTime 6 which can be downloaded from <http://www.apple.com/quicktime/>.

Recommendation:

If you use Quicktime, upgrade to Quicktime 6. If you are a web site that hosts the qtplugin.cab file you should upgrade to version 6.

You should never open attachments/webpages that come from unknown sources no matter how benign they may appear. Be wary of those that come from known sources.

You can set the "kill bit" for a known vulnerable ActiveX component by editing the registry. This will keep Internet Explorer from executing the vulnerable component. Directions for setting the kill bit on a are at:
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;q240797&>

You should consider the benefits and risks of each attachment file type or ActiveX components that you let into your organization. Attachment file types or ActiveX components that you do not need should be dropped at your perimeter mail gateway or proxy server. Attachments that you choose to forward on into your organization should be scanned for known malicious code using an antivirus product.

Common Vulnerabilities and Exposures (CVE) Information:

The Common Vulnerabilities and Exposures (CVE) project has assigned the following names to these issues. These are candidates for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

CAN-2002-0376 Apple QuickTime ActiveX v5.0.2 Buffer Overrun

@stake Vulnerability Reporting Policy:
<http://www.atstake.com/research/policy/>

@stake Advisory Archive:
<http://www.atstake.com/research/advisories/>

PGP Key:
http://www.atstake.com/research/pgp_key.asc

Copyright 2002 @stake, Inc. All rights reserved.

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

Version: PGP 7.0.3

iQA/AwUBPX5bY0e9kNifAm4yEQIH+QCdFToXSMrwI09izwdxGLEyUUKbTWEAoJbj
Z9cyqqB498EcNiXqMK/INQN3

VulnWatch: [VulnWatch] Apple QuickTime ActiveX v5.0.2 Buffer Overrun (a091002-1)

=MXuj

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

- **Previous message:** Michal Zalewski: "[VulnWatch] Strange Attractors and TCP/IP Sequence Number Analysis – One Year Later"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]