

[NEWS] Multiple Vulnerabilities Apple QuickTime/Darwin Streaming Server

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0096.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/23/03

To: list@securiteam.com

Date: 23 Jul 2003 11:30:12 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Multiple Vulnerabilities Apple QuickTime/Darwin Streaming Server

SUMMARY

Several vulnerabilities have been found in the Apple QuickTime/Darwin Streaming Server, including denial of service, web root traversal, and script source disclosure.

DETAILS

Affected system(s):

- * QuickTime/Darwin Streaming Server version 4.1.3 for MacOS X
- * QuickTime/Darwin Streaming Server version 4.1.3 for Win32
- * QuickTime/Darwin Streaming Server version 4.1.3 for Linux

Immune systems:

- * QuickTime/Darwin Streaming Server version 4.1.3g

Detailed analysis:

There are several vulnerabilities.

Securiteam: [NEWS] Multiple Vulnerabilities Apple QuickTime/Darwin Streaming Server

Denial of Service by HTTP Request for DOS Device Name

Affects: Darwin Streaming Server v4.1.3e and earlier (Win32 only)

CVE ID: CAN-2003-0421

Fixed: In version 4.1.3f (Win32)

Requesting a DOS device name (e.g. AUX) over HTTP (port 1220) will cause a denial of service on the server. An initial HTTP 404 response will be returned for the device request, but future requests will not be serviced.

For example:

```
GET /AUX HTTP/1.0
```

Denial of Service by Request for ../DOS Device Name

CVE ID: CAN-2003-0502

Affects: Darwin Streaming Server v4.1.3f and earlier (Win32 only)

Fixed: In version 4.1.3g (Win32)

This is a variant of CAN-2003-0421. A fix for CAN-2003-0421 was included in Streaming Server version, 4.1.3f, but further testing revealed that it was vulnerable to a variant where the device name was prefixed by dotdot slash (../), as in:

```
GET ../AUX HTTP/1.0
```

Denial of Service by HTTP Request for /view_broadcast.cgi Script

CVE ID: CAN-2003-0422

Affects: Darwin Streaming Server v4.1.3e and earlier (Win32 only)

Fixed: In version 4.1.3f (Win32)

Requesting the /view_broadcast.cgi script over HTTP (port 1220) will cause a denial of service on the server if the required request parameters are not sent. The connection will be closed midway through servicing the request and no new connections will be allowed to the server.

Example:

```
GET /view_broadcast.cgi HTTP/1.0
```

```
HTTP/1.0 200 OK
```

```
Content-Type: video/quicktime
```

```
rtsp://
```

```
^^ server drops connection
```

Source Disclosure via HTTP Request for /parse_xml.cgi Script

CVE ID: CAN-2003-0423

Affects: Darwin Streaming Server v4.1.3g and earlier

Fixed: No fix is available at this time. Apple is aware of this issue and they are investigating it further.

The source code of any file within the web root can be obtained by issuing a request for /parse_xml.cgi?filename=[file], where [file] is the file whose source code you wish to view.

Securiteam: [NEWS] Multiple Vulnerabilities Apple QuickTime/Darwin Streaming Server

This is only a serious risk if the administrator has installed custom scripts on Darwin Streaming Server that need to be protected.

Script Source Disclosure by Appending Special Characters

CVE ID: CAN-2003-0424

Affects: Darwin Streaming Server v4.1.3e and earlier (Win32 only)

Fixed: In version 4.1.3f (Win32)

The source code of any script can be obtained by appending the special characters %2e (period) or %20 (space) to an HTTP request for that script. For example, requesting /view_broadcast.cgi%2e will reveal the source code for that script.

Web Root Traversal and Arbitrary File Disclosure (Win32)

CVE ID: CAN-2003-0425

Affects: Darwin Streaming Server v4.1.3e and earlier (Win32 only)

Fixed: In version 4.1.3f (Win32)

Any file on the system can be retrieved by using three dots to break out of the web root. For example, requesting ../../qtusers will return the QuickTime user/password file.

Default Install Allows Remote User to Set Admin Password

CVE ID: CAN-2003-0426

Affects: Darwin Streaming Server v4.1.3e and earlier (Mac OS X only)

Fixed: In version 4.1.3f (Mac OS X)

When Darwin Streaming Server is first installed, the HTTP-based administration server (typically port 1220) presents a "Setup Assistant" page where the user is prompted to set a new administrator password. This would allow any remote user to connect and set up an administrator password before the server administrator has had a chance to do so.

Vendor status and information:

Apple – <<http://www.apple.com/>> <http://www.apple.com/>

The vendor has been notified and has released fixes for all but one of the issues, which is currently under investigation.

Solution:

Upgrade to version 4.1.3g or later of Darwin Streaming Server, which may be obtained as a free download from:

<<http://developer.apple.com/darwin/projects/streaming/>>
<http://developer.apple.com/darwin/projects/streaming/>

Please see the next section for detailed fix information.

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<<http://www.rapid7.com/advisories/R7-0015.html>>

Securiteam: [NEWS] Multiple Vulnerabilities Apple QuickTime/Darwin Streaming Server

<http://www.rapid7.com/advisories/R7-0015.html>

The information has been provided by <mailto:advisory@rapid7.com> Rapid7, Inc. Security Advisory.

=====

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.