

# [NEWS] Darwin Streaming Server Remote Denial of Service Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0062.html>

---

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

*Date:* 02/24/04

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

Date: 24 Feb 2004 10:10:35 +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>

-----

Darwin Streaming Server Remote Denial of Service Vulnerability

---

## SUMMARY

Darwin Streaming Server is server technology allowing for the streaming of QuickTime data to clients across the Internet using the industry standard RTP and RTSP protocols. Exploitation of a flaw in Apple Computer Inc's Darwin Streaming Server allows unauthenticated remote attackers to prevent legitimate usage.

## DETAILS

Vulnerable Systems:

\* Darwin Streaming Server version 4.1.3

The vulnerability specifically occurs upon parsing of DESCRIBE requests with specially crafted User-Agent fields. Making a request with a User-Agent field containing over 255 characters causes an assert error in CommonUtilitiesLib/StringFormatter.h line 97:

```
virtual void BufferIsFull(char* /*inBuffer*/, UInt32/*inBufferLen*/)
{
    Assert(0);
}
```

}

Successful exploitation disrupts further content streaming capabilities.

Vendor Status:

This is fixed in Security Update 2004-02-23 available for Mac OS X 10.3.2 Server and Mac OS X 10.2.8 Server. The update and further information is available from Apple's Support site at: <<http://www.apple.com/support/>>  
<http://www.apple.com/support/>

CVE Information:

The Common Vulnerabilities and Exposures (CVE) project has assigned the CAN-2004-0169 to this issue. This is a candidate for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

Disclosure timeline:

- December 8, 2003 – Exploit acquired by iDEFENSE
- January 29, 2004 – iDEFENSE clients notified
- January 29, 2004 – Initial vendor notification
- January 29, 2004 – Vendor response received
- February 23, 2004 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by  
<<mailto:idlabs-advisories@idefense.com>> iDEFENSE.

The original article can be found at:

<<http://www.idefense.com/application/poi/display?id=75&type=vulnerabilities>>  
<http://www.idefense.com/application/poi/display?id=75&type=vulnerabilities>.

=====

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](mailto:list-unsubscribe@securiteam.com)  
In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.