

[NT] Adobe Flash Media Server 2 Memory Corruption Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00031.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 13 Feb 2008 09:24:22 +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>

Adobe Flash Media Server 2 Memory Corruption Vulnerability

SUMMARY

<<http://www.adobe.com/products/flashmediaserver/>> Adobe Flash Media Server is "an application server for Flash based applications. It provides an environment to run interactive media applications, as well as audio and video streaming functionality". Remote exploitation of a memory corruption vulnerability in Adobe Systems Inc.'s Flash Media Server 2 could allow an unauthenticated attacker to execute arbitrary code with SYSTEM privileges.

DETAILS

Vulnerable Systems:

- * Flash Media Server 2 version 2.0.4

Immune Systems:

- * Flash Media Server 2 version 2.0.5

The Flash Media Server contains a component called the Edge server, which listens on TCP ports 1935 and 19350 for incoming connections. This port is the primary port used for client/server communication. The Edge server speaks the Real Time Message Protocol, or RTMP, a proprietary binary

[NT] Adobe Flash Media Server 2 Memory Corruption Vulnerability

protocol developed by Adobe.

This vulnerability exists within the code responsible for parsing RTMP messages. A certain sequence of requests can lead to an area of memory being used after it has been released. This leads to the execution of arbitrary code.

Analysis:

Exploitation of this vulnerability results in the execution of arbitrary code with SYSTEM level privileges. In order to exploit this vulnerability, an attacker only needs the ability to connect to the target server on TCP port 1935 or 19350.

Unsuccessful attempts at exploitation will likely result in the Edge server crashing. After crashing, the Edge server will be restarted automatically. This gives an attacker an unlimited number of attempts at exploitation.

V. WORKAROUND

iDefense is currently unaware of any workarounds for this issue.

Vendor response:

Adobe has addressed this vulnerability by releasing version 2.0.5 of Flash Media Server. For more information, consult their bulletin at the following URL:

<<http://www.adobe.com/support/security/bulletins/apsb08-03.html>>
<http://www.adobe.com/support/security/bulletins/apsb08-03.html>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6148>>
CVE-2007-6148

Disclosure Timeline:

11/27/2007 – Initial vendor notification
11/27/2007 – Initial vendor response
02/12/2008 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense Labs.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=663>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=663>

=====

[NT] Adobe Flash Media Server 2 Memory Corruption Vulnerability

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@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====
=====

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.