

[NEWS] MPlayer "ASF" File Handling Multiple Integer Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-02/msg00073.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 26 Feb 2006 13:42:42 +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>

MPlayer "ASF" File Handling Multiple Integer Overflows

SUMMARY

" <<http://www.mplayerhq.hu/>> MPlayer is a movie player which runs on many systems"

Improper handling of ASF files allows attackers to DoS MPlayer.

DETAILS

Vulnerable Systems:

- * MPlayer version 1.0pre7
- * MPlayer version 1.0pre7try2

Immune Systems:

- * MPlayer version 1.89
- * MPlayer version 1.90

Multiple Integer overflow exists with the way that MPlayer works with ASF. The problem exists in libmpdemux/demuxer.h header file with the function `new_demux_packet()`. And with the C file of libmpdemux/demux_asf.c the function

[NEWS] MPlayer "ASF" File Handling Multiple Integer Overflows

demux_asf_read_packet().

The problem happen when allocating memory to copy data from an .asf file.

An attacker can exploit this vulnerability to DoS MPlayer by using a crafted .ASF file with a large value in the packet length field.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0579>>
CVE-2006-0579

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jaervosz@xxxxxxxxxx>> Sune Kloppenborg Jeppesen.

The original article can be found at:

<http://bugs.gentoo.org/show_bug.cgi?id=122029>
http://bugs.gentoo.org/show_bug.cgi?id=122029

=====

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@xxxxxxxxxxxxxxxx

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

=====
=====

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.