

# [NEWS] MPlayer Buffer Overflow Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-02/msg00017.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 7 Feb 2008 14:40:28 +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 Buffer Overflow Vulnerability

---

### SUMMARY

The <<http://www.mplayerhq.hu/>> MPlayer package [1] is vulnerable to a buffer overflow attack, which can be exploited by malicious remote attackers. The vulnerability is due to MPlayer not properly sanitizing certain tags on a FLAC file before using them to index an array on the stack. This can be exploited to execute arbitrary commands by opening a specially crafted file.

The <<http://xinehq.de/>> Xine package [2], and probably other packages based on <<http://www.mplayerhq.hu/design7/projects.html>> MPlayer [3], are vulnerable to this attack too.

### DETAILS

#### Vulnerable Systems:

- \* MPlayer version 1.0rc2 and SVN before r25917 (Tue Jan 29 22:00:58 2008 UTC)
- \* Xine-lib version 1.1.10

#### Immune Systems:

- \* MPlayer SVN HEAD after r25917

## [NEWS] MPlayer Buffer Overflow Vulnerability

\* MPlayer version 1.0rc2 + security patches

Vendor response:

A fix for this problem was committed to SVN on the

<[http://svn.mplayerhq.hu/mplayer/trunk/libmpdemux/demux\\_audio.c?r1=25911&r2=25917](http://svn.mplayerhq.hu/mplayer/trunk/libmpdemux/demux_audio.c?r1=25911&r2=25917)> MPlayer project [4]. Users of affected MPlayer versions should download a

<[http://www.mplayerhq.hu/MPlayer/patches/demux\\_audio\\_fix\\_20080129.diff](http://www.mplayerhq.hu/MPlayer/patches/demux_audio_fix_20080129.diff)> patch [5] for MPlayer 1.0rc2 or update to the latest version if they are using SVN.

Technical details:

The vulnerability was found in the following code, used to parse FLAC comments inside MPlayer:

```
libmpdemux/demux_audio.c
206 case FLAC_VORBIS_COMMENT:
207 {
208 /* For a description of the format please have a look at */
209 /* http://www.xiph.org/vorbis/doc/v-comment.html */
210
211 uint32_t length, comment_list_len;
212 (1) char comments[blk_len];
213 uint8_t *ptr = comments;
214 char *comment;
215 int cn;
216 char c;
217
218 if (stream_read (s, comments, blk_len) == blk_len)
219 {
220 (2) length = AV_RL32(ptr);
221 ptr += 4 + length;
222
223 comment_list_len = AV_RL32(ptr);
224 ptr += 4;
225
226 cn = 0;
227 for (; cn < comment_list_len; cn++)
228 {
229 length = AV_RL32(ptr);
230 ptr += 4;
231
232 comment = ptr;
233 (3) c = comment[length];
234 comment[length] = 0;
...

```

We can see in (2) that the length variable is being loaded from a position on the file stream, and then used without any validation to index the comment buffer, that was allocated from the stack in (1). This causes a stack corruption, and possibly allows code execution (e.g. modifying the value of the length variable, that is also on the stack).

[NEWS] MPlayer Buffer Overflow Vulnerability

Example Attack Scenario:

- 1) The user receives an email with an attachment called e.g. goodmusic.flac.
- 2) The user opens the file with MPlayer or another vulnerable software.
- 3) This causes a stack corruption and malicious code execution on the user computer.

Report Timeline

- \* 2007-12-18: Core Security Technologies notifies the MPlayer team of the vulnerability (no reply received).
- \* 2008-01-04: A new notification of the vulnerability was sent to the MPlayer team (no reply received).
- \* 2008-01-18: A new notification of the vulnerability was sent to the MPlayer team.
- \* 2008-01-18: The MPlayer team asked Core Security Technologies for technical description of the vulnerability.
- \* 2008-01-22: Technical details was sent to MPlayer team by Core Security Technologies.
- \* 2008-01-28: MPlayer notified Core Security Technologies that a fix had been produced.
- \* 2008-02-04: CORE-2007-1218 advisory was published.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0486>>  
 CVE-2008-0486

ADDITIONAL INFORMATION

The information has been provided by <<mailto:advisories@xxxxxxxxxxxxxxxxxx>>  
 CORE Security Technologies Advisories.

The original article can be found at:

<<http://www.coresecurity.com/?action=item&id=2103>>  
<http://www.coresecurity.com/?action=item&id=2103>

=====

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@xxxxxxxxxxxxxxxxxx

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

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

[NEWS] MPlayer Buffer Overflow Vulnerability

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.