Back to list | Post reply

[TKADV2009-004] FFmpeg Type Conversion Vulnerability Jan 28 2009 09:07PM
Tobias Klein (tk trapkit de)

Please find attached a detailed advisory of the vulnerability.

Alternatively, the advisory can also be found at:
http://www.trapkit.de/advisories/TKADV2009-004.txt
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Advisory: FFmpeg Type Conversion Vulnerability
Advisory ID: TKADV2009-004
Revision: 1.0
Release Date: 2009/01/28
Last Modified: 2009/01/28
Date Reported: 2009/01/25
Author: Tobias Klein (tk at trapkit.de)
Affected Software: FFmpeg SVN trunk < revision 16846
Remotely Exploitable: Yes
Locally Exploitable: No
Vendor URL: http://ffmpeg.mplayerhq.hu/
Vendor Status: Vendor has released an updated version
Patch development time: 3 days

======================
Vulnerability Details:
======================

FFmpeg contains a type conversion vulnerability while parsing malformed 4X
movie files. The vulnerability may be exploited by a (remote) attacker to
execute arbitrary code in the context of FFmpeg or an application using
the FFmpeg library.

FFmpeg is used by a lot of popular software projects like VLC media player
[1], Mplayer [2], Perian [3] and Xine [4].

==================
Technical Details:
==================

Source code file: libavformat/4xm.c

[..]
93 static int fourxm_read_header(AVFormatContext *s,
94 AVFormatParameters *ap)
95 {
..
103 [8] int current_track = -1;
..
106 [9] fourxm->track_count = 0;
107 [10] fourxm->tracks = NULL;
..
160 } else if (fourcc_tag == strk_TAG) {
161 /* check that there is enough data */
162 if (size != strk_SIZE) {
163 av_free(header);
164 return AVERROR_INVALIDDATA;
165 }
166 [1] current_track = AV_RL32(&header[i + 8]);
167 [2] if (current_track + 1 > fourxm->track_count) {
168 fourxm->track_count = current_track + 1;
169 if((unsigned)fourxm->track_count >= UINT_MAX /
sizeof(AudioTrack))
170 return -1;

```
171 [3] fourxm->tracks = av_realloc(fourxm->tracks,
172 fourxm->track_count * sizeof(AudioTrack));
173 if (!fourxm->tracks) {
174 av_free(header);
175 return AVERROR(ENOMEM);
176 }
177 }
178 [4] fourxm->tracks[current_track].adpcm = AV_RL32(&header[i + 12]);
179 [5] fourxm->tracks[current_track].channels = AV_RL32(&header[i + 36]);
180 [6] fourxm->tracks[current_track].sample_rate = AV_RL32(&header[i+40]);
181 [7] fourxm->tracks[current_track].bits = AV_RL32(&header[i + 44]);
[..]
```

[1] The signed int variable "current_track" (see [8]) is filled with user supplied data from the media file
[2] This statement checks if the user controlled value of "current_track" is greater than "fourxm->track_count". The variable "fourxm->track_count" is initialized with 0 (see [9]). By supplying a value >= 0x80000000 for "current_track" it is possible to cause a change in sign that results in "current_track" being negative. If "current_track" is negative, the if statement will always return false and the buffer allocation in [3] will never be reached.
[4] As "fourxm->tracks" is initialized with NULL (see [10]) and line 171 is never reached this leads to an exploitable NULL pointer dereference. It is possible to write 4 bytes of user controlled data to the memory location "NULL + current_track". As the value of "current_track" is also controlled by the user it is possible to write 4 bytes of arbitrary data at a wide range of memory addresses.
[5] See [4]
[6] See [4]
[7] See [4]

A malicious party may exploit this issue to execute arbitrary code by overwriting a sensitive memory location (such as a GOT/IAT entry, a return address, buffer length or boolean variable).

=========
Solution:
=========

Upgrade to FFmpeg SVN trunk >= revision 16846

========
History:
========

2009/01/25 - FFmpeg maintainers notified
2009/01/27 - Patch developed by FFmpeg maintainers
2009/01/28 - Public disclosure of vulnerability details by FFmpeg maintainers
2009/01/28 - Release date of this security advisory

========
Credits:
========

Vulnerability found and advisory written by Tobias Klein.

===========
References:
===========

[1] http://www.videolan.org/
[2] http://www.mplayerhq.hu/
[3] http://www.perian.org/
[4] http://www.xinehq.de/
[5] http://git.ffmpeg.org/?p=ffmpeg;a=commitdiff;h=72e715fb798f2cb79fd24a6d2eaeafb7c6eeda17
[6] http://www.trapkit.de/advisories/TKADV2009-004.txt

========
Changes:
========

Revision 0.1 - Initial draft release to the vendor

Revision 1.0 - Public release

==========
Disclaimer:
==========

The information within this advisory may change without notice. Use
of this information constitutes acceptance for use in an AS IS
condition. There are no warranties, implied or express, with regard
to this information. In no event shall the author be liable for any
direct or indirect damages whatsoever arising out of or in connection
with the use or spread of this information. Any use of this
information is at the user's own risk.

==================
PGP Signature Key:
==================

http://www.trapkit.de/advisories/tk-advisories-signature-key.asc

-----BEGIN PGP SIGNATURE-----
Version: GnuPG

iD8DBQFJgMdJkXxgcAIbhEERAgm3AJ4lPK2ww18QOAgLM+MH8QJMT28lWwCdFQ48
fzlqRUvio8oIYJ4Nls+kTF4=
=KMsk
-----END PGP SIGNATURE-----

[reply]