

[UNIX] Mpg123 Buffer Overflow Due To Bugs In Header Checks Code

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0017.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/07/04

To: list@securiteam.com

Date: 7 Sep 2004 20:26:51 +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>

Mpg123 Buffer Overflow Due To Bugs In Header Checks Code

SUMMARY

<<http://www.mpg123.de/>> mpg123 reads one or more files (or standard input if "-" is specified) or URLs and plays them on the audio device (default) or outputs them to stdout.

Due to buggy code when parsing mpeg layer 2 headers it is possible to cause mpg123 to fail when parsing the mpeg file headers.

DETAILS

Vulnerable Systems:

- * mpg123 version 0.59r and 0.59s as well, all platforms

Immune Systems:

- * mpg123 with latest patch from Debian CVS

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0805>>
CAN-2004-0805

Securiteam: [UNIX] Mpg123 Buffer Overflow Due To Bugs In Header Checks Code

A malicious formatted mp3/2 causes mpg123 to fail header checks. This may allow arbitrary code to be executed with the privilege of the user trying to play the mp3. The impact of such a vulnerability is that any movie file sent to a vulnerable system can easily execute code and spawn a shell (for example). Since mpg123 is present on most Unix and Linux systems, this leaves a rather large quantity of users vulnerable.

Disclosure Timeline

16/08/2003 – Vulnerability discovered

06/09/2003 – Public advisory release

Patch Availability:

The author has been contacted but no reply was received. However, a patch is provided by Daniel Kobras, the Debian mpg123 package maintainer. The patch should apply to the source version of mpg123 and therefore it is listed below:

----- Begin Code

Index: layer2.c

RCS file: /home/kobras/cvsroot/debian/mpg123/layer2.c,v

retrieving revision 1.1.1.1

diff -u -r1.1.1.1 layer2.c

--- layer2.c 1999/02/10 12:13:06 1.1.1.1

+++ layer2.c 2004/09/02 21:43:58

@@ -265,6 +265,11 @@

fr->jsbound = (fr->mode == MPG_MD_JOINT_STEREO) ?

(fr->mode_ext<<2)+4 : fr->II_sblimit;

+ if (fr->jsbound > fr->II_sblimit) {

+ fprintf(stderr, "Truncating stereo boundary to sideband
limit.\n");

+ fr->jsbound=fr->II_sblimit;

+ }

+

if(stereo == 1 || single == 3)

single = 0;

----- End Code

ADDITIONAL INFORMATION

The information has been provided by <<mailto:dante@alighieri.org>> Davide Del Vecchio.

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

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

Securiteam: [UNIX] Mpg123 Buffer Overflow Due To Bugs In Header Checks Code

=====
=====

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.