

[NEWS] Multiple Vendor FLAC Library Multiple Integer Overflow Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-10/msg00022.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 15 Oct 2007 08:13:25 +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>

Multiple Vendor FLAC Library Multiple Integer Overflow Vulnerabilities

SUMMARY

<<http://flac.sourceforge.net/>> Free Lossless Audio Codec (FLAC) is "a popular file format for audio data compression. AOL Corp.'s Winamp media player has support for the FLAC format". Remote exploitation of multiple integer overflow vulnerabilities in libFLAC, as included with various vendor's software distributions, allows attackers to execute arbitrary code in the context of the currently logged in user.

DETAILS

Vulnerable Systems:

- * libFLAC version 1.2.0

Immune Systems:

- * libFLAC version 1.2.1

These vulnerabilities specifically exist in the handling of malformed FLAC media files. In each case, an integer overflow can occur while calculating the amount of memory to allocate. As such, insufficient memory is allocated for the data that is subsequently read in from the file, and a

[NEWS] Multiple Vendor FLAC Library Multiple Integer Overflow Vulnerabilities

heap based buffer overflow occurs.

Analysis:

Exploitation allows remote attackers to execute arbitrary code in the context of the user attempting to play the media file. Exploitation requires that an attacker persuade a targeted user into opening a malformed FLAC file.

Workaround:

For Winamp users, it is possible to remove support for the FLAC file format by uninstalling the FLAC input plug-in.

Vendor response:

The FLAC maintainers have released version 1.2.1 of FLAC to address these vulnerabilities. AOL Corp. has addressed this vulnerability in version 5.5 of Winamp. For more information see the FLAC change log at the following URL: <<http://flac.sourceforge.net/changelog.html>>
<http://flac.sourceforge.net/changelog.html>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4619>>
CVE-2007-4619

Disclosure Timeline:

08/29/2007 – Initial vendor notification
08/29/2007 – Initial vendor response
10/11/2007 – 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=608>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=608>

=====

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:

[NEWS] Multiple Vendor FLAC Library Multiple Integer Overflow Vulnerabilities

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.