Sisyphus-wang / **CVE-2025-56226.md**

Last active last month

Code Revisions 7

libsndfile: sndfile-convert MP3 encoder memory leak (CVE-2025-56226) (Fixed)

CVE-2025-56226.md

libsndfile: sndfile-convert MP3 encoder memory leak (CVE-2025-56226) (Fixed)

Summary

ibsndfile versions 1.1.0 through 1.2.2 were affected by a memory leak in the sndfile-convert utility when encoding MP3 files.

The leak occurs in the error handling path of the MP3 encoder initialization logic, where resources allocated by lame_init() are not released when an early return is triggered.

This issue has already been fixed in the libsndfile project.

This document is provided for historical reference and traceability only.

Affected Component

Project: libsndfile

Tool: sndfile-convert

File: src/mpeg_l3_encode.c

Function: mpeg_l3_encoder_init

Root Cause Analysis (Confirmed)

The root cause of the memory leak is an incomplete initialization sequence combined with early error returns.

In libsndfile/src/mpeg_l3_encode.c, the encoder context is allocated via lame_init(), but the corresponding cleanup callback (psf->codec_close) is not set immediately after successful allocation.

Relevant code path (pre-fix):

```
if (! (pmpeg->lamef = lame_init ()))
    return SFE_MALLOC_FAILED ;
/* ... */

if (lame_set_out_samplerate (pmpeg->lamef, psf->sf.samplerate) < 0)
    return SFE_MPEG_BAD_SAMPLERATE ;

/* codec_close is set only here */
psf->sf.seekable    = 0 ;
psf->codec_close    = mpeg_l3_encoder_close ;
psf->byterate       = mpeg_l3_encoder_byterate ;
psf->datalength     = 0 ;

return 0 ;
```

Failure scenario

1. lame_init() successfully allocates encoder resources.
2. lame_set_out_samplerate() fails due to an unsupported sample rate.
3. Function returns SFE_MPEG_BAD_SAMPLERATE.
4. Cleanup callback (psf->codec_close) has not yet been set.
5. Allocated encoder resources are not released, resulting in a memory leak.

Fix Description

This issue has been resolved in the official libsndfile repository.

ref:libsndfile/libsndfile#1090