mackron / dr_libs Public

Code Issues 8 Pull requests Discussions Actions Projects Se

Commit 663239a

mackron committed 4 days ago

dr_flac: Fix a possible overflow error when parsing picture metadata.

Public issue #298

master

1 parent 0b12cb5 commit 663239a

1 file changed +11 -3

Top

Filter files...

dr_flac.h

Search within code

dr_flac.h

```
@@ -1,6 +1,6 @@
 /*
 FLAC audio decoder. Choice of public domain or MIT-0. See license
 statements at the end of this file.
-dr_flac - v0.13.3 - 2026-01-17
+dr_flac - v0.13.4 - TBD

 David Reid - mackron@gmail.com

@@ -126,7 +126,7 @@ extern "C" {

 #define DRFLAC_VERSION_MAJOR     0
```

```
128  128    #define DRFLAC_VERSION_MINOR      13
129         - #define DRFLAC_VERSION_REVISION  3
     129    + #define DRFLAC_VERSION_REVISION  4
130  130    #define DRFLAC_VERSION_STRING    DRFLAC_XSTRINGIFY(DRFLAC_VERSION_MAJOR)
            "." DRFLAC_XSTRINGIFY(DRFLAC_VERSION_MINOR) "."
            DRFLAC_XSTRINGIFY(DRFLAC_VERSION_REVISION)
131  131
132  132    #include <stddef.h> /* For size_t. */
       ↓    @@ -6747,13 +6747,18 @@ static drflac_bool32
       ↑    drflac__read_and_decode_metadata(drflac_read_proc onRead, d
6747 6747                       blockSizeRemaining -= 4;
6748 6748                       metadata.data.picture.mimeLength =
            drflac__be2host_32(metadata.data.picture.mimeLength);
6749 6749
     6750    +                  if (blockSizeRemaining <
            metadata.data.picture.mimeLength) {
     6751    +                      result = DRFLAC_FALSE;
     6752    +                      goto done_flac;
     6753    +                  }
     6754    +
6750 6755                       pMime =
            (char*)drflac__malloc_from_callbacks(metadata.data.picture.mimeLength + 1,
            pAllocationCallbacks); /* +1 for null terminator. */
6751 6756                       if (pMime == NULL) {
6752 6757                           result = DRFLAC_FALSE;
6753 6758                           goto done_flac;
6754 6759                       }
6755 6760
6756        - if (blockSizeRemaining <
            metadata.data.picture.mimeLength || onRead(pUserData, pMime,
            metadata.data.picture.mimeLength) != metadata.data.picture.mimeLength) {
     6761    +                  if (onRead(pUserData, pMime,
            metadata.data.picture.mimeLength) != metadata.data.picture.mimeLength) {
6757 6762                           result = DRFLAC_FALSE;
6758 6763                           goto done_flac;
6759 6764                       }
       ↓    @@ -12169,6 +12174,9 @@ DRFLAC_API drflac_bool32
       ↑    drflac_next_cuesheet_track(drflac_cuesheet_track_iterat
12169 12174    /*
12170 12175    REVISION HISTORY
```

```
12171  12176    ================
       12177  + v0.13.4 - TBD
       12178  +   - Fix a possible overflow error when parsing picture metadata.
       12179  +
12172  12180    v0.13.3 - 2026-01-17
12173  12181      - Fix a compiler compatibility issue with some inlined assembly.
12174  12182      - Fix a compilation warning.
```

Comments 0

Please sign in to comment.