mackron / dr_libs Public

Code Issues 8 Pull requests Discussions Actions Projects Se

Commit 4f5a4cd

mackron committed 4 days ago

dr_flac: Add some bounds checking when parsing metadata.

Public issue #298

1 parent b8fddd9 commit 4f5a4cd

1 file changed +21 -4

Top

Filter files…

dr_flac.h

Search within code

dr_flac.h

```
@@ -6430,11 +6430,22 @@ static drflac_bool32 drflac__read_and_decode_metadata(drflac_read_proc onRead, d
6430 6430         We want to keep track of the byte position in the stream of the seektable. At the time of calling this function we know that
6431 6431         we'll be sitting on byte 42.
6432 6432         */
6433      -      drflac_uint64 runningFilePos = 42;
6434      -      drflac_uint64 seektablePos   = 0;
6435      -      drflac_uint32 seektableSize  = 0;
     6433 +      drflac_uint64 runningFilePos   = 42;
     6434 +      drflac_uint64 seektablePos     = 0;
     6435 +      drflac_uint32 seektableSize    = 0;
     6436 +      drflac_int64  fileSize         = 0;
```

```
                6437 +     drflac_bool32 hasKnownFileSize = DRFLAC_FALSE;
6436            6438
6437                -     (void)onTell;
                6439 +     /* We'll be doing some memory allocations here against untrusted data. We'll do a basic validation check that they don't exceed the size of the file. */
                6440 +     if (onTell != NULL && onSeek != NULL) {
                6441 +         if (onSeek(pUserData, 0, DRFLAC_SEEK_END)) {
                6442 +             if (onTell(pUserData, &fileSize)) {
                6443 +                 hasKnownFileSize = DRFLAC_TRUE;
                6444 +             }
                6445 +
                6446 +             onSeek(pUserData, runningFilePos, DRFLAC_SEEK_SET);
                6447 +         }
                6448 +     }
6438            6449
6439            6450         for (;;) {
6440            6451             drflac_metadata metadata;
                    ⇕       @@ -6444,6 +6455,11 @@ static drflac_bool32 drflac__read_and_decode_metadata(drflac_read_proc onRead, d
6444            6455             if (drflac__read_and_decode_block_header(onRead, pUserData, &isLastBlock, &blockType, &blockSize) == DRFLAC_FALSE) {
6445            6456                 return DRFLAC_FALSE;
6446            6457             }
                6458 +
                6459 +             if (hasKnownFileSize && (blockSize > ((drflac_uint64)fileSize - runningFilePos))) {
                6460 +                 return DRFLAC_FALSE;    /* Block size exceeds the size of the file. */
                6461 +             }
                6462 +
6447            6463             runningFilePos += 4;
6448            6464
6449            6465             metadata.type = blockType;
                    ⇕       @@ -12180,6 +12196,7 @@ DRFLAC_API drflac_bool32 drflac_next_cuesheet_track(drflac_cuesheet_track_iterat
12180           12196     REVISION HISTORY
12181           12197     ================
12182           12198     v0.13.4 - TBD
                12199 +   - Add a bounds check when allocating memory during metadata processing.
```

```
12183   12200       - Fix a possible overflow error when parsing picture metadata.
12184   12201
12185   12202     v0.13.3 - 2026-01-17
```

Comments 0