mackron / dr_libs Public

Code Issues 8 Pull requests Discussions Actions Projects Se

Commit fefced4

mackron committed 4 days ago

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

Public issue #298

master

1 parent 0e407e8 commit fefced4

1 file changed +6 -1

Top

Filter files...

dr_flac.h

Search within code

dr_flac.h

```
@@ -6774,13 +6774,18 @@ static drflac_bool32 drflac__read_and_decode_metadata(drflac_read_proc onRead, d
6774 6774                     blockSizeRemaining -= 4;
6775 6775                     metadata.data.picture.descriptionLength = drflac__be2host_32(metadata.data.picture.descriptionLength);
6776 6776
     6777 +                   if (blockSizeRemaining < metadata.data.picture.descriptionLength) {
     6778 +                       result = DRFLAC_FALSE;
     6779 +                       goto done_flac;
     6780 +                   }
     6781 +
```

```
6777  6782                        pDescription =
      (char*)drflac__malloc_from_callbacks(metadata.data.picture.descriptionLength
      + 1, pAllocationCallbacks); /* +1 for null terminator. */
6778  6783                        if (pDescription == NULL) {
6779  6784                            result = DRFLAC_FALSE;
6780  6785                            goto done_flac;
6781  6786                        }
6782  6787
6783        -                     if (blockSizeRemaining <
      metadata.data.picture.descriptionLength || onRead(pUserData, pDescription,
      metadata.data.picture.descriptionLength) !=
      metadata.data.picture.descriptionLength) {
      6788  +                     if (onRead(pUserData, pDescription,
      metadata.data.picture.descriptionLength) !=
      metadata.data.picture.descriptionLength) {
6784  6789                            result = DRFLAC_FALSE;
6785  6790                            goto done_flac;
6786  6791                        }
```

Comments 0

Please sign in to comment.