

Commit **5f6d0aa** **cary-ilm** committed last week

PXR24: reject zlib output that does not match packed payload size ([#2310](#))

\* PXR24: reject zlib output that does not match packed payload size

PXR24 stores zlib-compressed packed channel data (e.g. 3 bytes/sample for float), while chunk `unpacked_size` is the native layout (4 bytes/sample). After inflate, validate the decompressed length against the packed byte count derived from the same geometry as encode/decode, not `unpacked_size`.

A truncated-but-valid zlib stream previously produced success with a short `actual_out` while the decoder advanced through scratch as if the full packed block were present, reading uninitialized heap into pixels.

Add `pxr24_packed_zlib_size()` (aligned with `apply_pxr24_impl`) and require `outSize ==` that value after `exr_uncompress_buffer()` succeeds.

Analysis and solution with the the help of Cursor / Claude Opus 4.5

Signed-off-by: Cary Phillips <cary@ilm.com>

\* replace comparison to `uncompressed_size` with `outSize`

A simpler solution: remove `pxr24_packed_zlib_size()` entirely detect corrupt chunks by comparing against `outSize` instead of `uncompressed_size`.

Signed-off-by: Cary Phillips <cary@ilm.com>

-----

Signed-off-by: Cary Phillips <cary@ilm.com>

[RB-3.4](#) + [release](#) · [v3.4.8](#) [v3.4.8-rc](#)

1 parent [7c51321](#) commit 5f6d0aa

2 files changed +8 -4 lines changed

↑ Top ⚙

🔍 Filter files...

src/lib/OpenEXRCore

compression.c

internal\_pxr24.c

2 files changed +8 -4 lines changed

🔍 Search within code



src/lib/OpenEXRCore/compression.c



```

↑... @@ -201,7 +201,11 @@ exr_uncompress_buffer (
201 201     }
202 202     else if (res == LIBDEFLATE_SHORT_OUTPUT)
203 203     {
204 -        /* TODO: is this an error? */
204 +        /* Decompression succeeded; *actual_out is the byte count. This is
205 +        * not an error when out_bytes_avail exceeds the true uncompressed
206 +        * size (e.g. PXR24/ZIP use padded scratch buffers). Callers that
207 +        * need an exact payload size must compare *actual_out (see e.g.
208 +        * undo_pxr24_impl). */
205 209         return EXR_ERR_SUCCESS;
206 210     }
207 211     return EXR_ERR_CORRUPT_CHUNK;

```



src/lib/OpenEXRCore/internal\_pxr24.c



```

↑... @@ -320,7 +320,7 @@ undo_pxr24_impl (
320 320     ptr[3] = lastIn;
321 321     lastIn += w;
322 322
323 -        if (nDec + nBytes > uncompressed_size)
323 +        if (nDec + nBytes > outSize)
324 324         return EXR_ERR_CORRUPT_CHUNK;
325 325
326 326         for (int x = 0; x < w; ++x)

```



```

@@ -347,7 +347,7 @@ undo_pxr24_impl (

```

```
347 347 ptr[1] = lastIn;
348 348 lastIn += w;
349 349
350 - if (nDec + nBytes > uncompressed_size)
350 + if (nDec + nBytes > outSize)
351 351 return EXR_ERR_CORRUPT_CHUNK;
352 352
353 353 for (int x = 0; x < w; ++x)
@@ -374,7 +374,7 @@ undo_pxr24_impl (
374 374 ptr[2] = lastIn;
375 375 lastIn += w;
376 376
377 - if (nDec + (uint64_t) (w * 3) > uncompressed_size)
377 + if (nDec + (uint64_t) (w * 3) > outSize)
378 378 return EXR_ERR_CORRUPT_CHUNK;
379 379
380 380 for (int x = 0; x < w; ++x)
```

## Comments 0



Please [sign in](#) to comment.