

Commit 3827998

 **cary-ilm** committed 3 weeks ago

Fix integer overflow in htj2k decode with width > 32767 (#2291)

Loop iterators need to be int32_t, not int16_t.

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

 RB-3.4 + release ·  v3.4.9-rc ... v3.4.7-rc


1 parent [42a397a](#) commit 3827998 

 **1 file changed** +4 -4 lines changed

 Top 

 Filter files...

▼  src/lib/OpenEXRCore

 internal_ht.cpp

 **1 file changed** +4 -4 lines changed

 Search within code



▼ src/lib/OpenEXRCore/internal_ht.cpp 

```

@@ -257,7 +257,7 @@ ht_undo_impl (
257 257             EXR_PIXEL_HALF)
258 258             {
259 259             int16_t* channel_pixels = (int16_t*) line_pixels;
260 -             for (int16_t p = 0;
+             for (int32_t p = 0;
261 261                 p < decode->channels[file_c].width;
262 262                 p++)
263 263             {
@@ -267,7 +267,7 @@ ht_undo_impl (
267 267             else

```

268	268		{
269	269		int32_t* channel_pixels = (int32_t*) line_pixels;
270	-		for (int16_t p = 0;
270	+		for (int32_t p = 0;
271	271		p < decode->channels[file_c].width;
272	272		p++)
273	273		{
		⌵	@@ -299,7 +299,7 @@ ht_undo_impl (
		⌶	
299	299		{
300	300		int16_t* channel_pixels =
301	301		(int16_t*) (line_pixels +
			cs_to_file_ch[c].raster_line_offset);
302	-		for (int16_t p = 0; p < decode->channels[file_c].width;
302	+		for (int32_t p = 0; p < decode->channels[file_c].width;
303	303		p++)
304	304		{
305	305		*channel_pixels++ = cur_line->i32[p];
		⌵	@@ -309,7 +309,7 @@ ht_undo_impl (
		⌶	
309	309		{
310	310		int32_t* channel_pixels =
311	311		(int32_t*) (line_pixels +
			cs_to_file_ch[c].raster_line_offset);
312	-		for (int16_t p = 0; p < decode->channels[file_c].width;
312	+		for (int32_t p = 0; p < decode->channels[file_c].width;
313	313		p++)
314	314		{
315	315		*channel_pixels++ = cur_line->i32[p];
		⌵	

Comments 0



Please [sign in](#) to comment.