

pnggroup / libpng Public

<> Code Issues 149 Pull requests 28 Discussions Actions Projects

Commit a3a2144



Oblivionsage authored and ctruta committed 2 weeks ago · ✓ 4/4



fix: Initialize tail bytes in trans_alpha buffers

Although the arrays `info_ptr->trans_alpha` and `png_ptr->trans_alpha` are allocated 256 bytes, only `num_trans` bytes are copied. The remaining entries were left uninitialized. Set them to 0xff (fully opaque) before copying, which matches the conventional treatment of entries beyond `num_trans`.

This is a follow-up to the previous use-after-free fix.

Reported-by: Cosmin Truta <ctruta@gmail.com>
Reviewed-by: Cosmin Truta <ctruta@gmail.com>
Signed-off-by: Cosmin Truta <ctruta@gmail.com>

libpng18 · v1.6.56

1 parent [bf7fefe](#) commit a3a2144

1 file changed +6 -1 lines changed

↑ Top ⚙️

Filter files...



pngset.c

1 file changed +6 -1 lines changed

Search within code



pngset.c



```

@@ -1159,9 +1159,13 @@ png_set_tRNS(png_structrp png_ptr, png_inforp
info_ptr,
1159 1159
1160 1160     if (num_trans > 0 && num_trans <= PNG_MAX_PALETTE_LENGTH)
1161 1161     {
1162 -        /* Allocate info_ptr's copy of the transparency data. */
1162 +        /* Allocate info_ptr's copy of the transparency data.

```

1163	+	* Initialize all entries to fully opaque (0xff), then overwrite
1164	+	* the first num_trans entries with the actual values.
1165	+	*/
1163	1166	info_ptr->trans_alpha = png_voidcast(png_bytep,
1164	1167	png_malloc(png_ptr, PNG_MAX_PALETTE_LENGTH));
1168	+	memset(info_ptr->trans_alpha, 0xff, PNG_MAX_PALETTE_LENGTH);
1165	1169	memcpy(info_ptr->trans_alpha, trans_alpha, (size_t)num_trans);
1166	1170	info_ptr->free_me = PNG_FREE_TRNS;
1167	1171	info_ptr->valid = PNG_INFO_TRNS;
		@@ -1177,6 +1181,7 @@ png_set_tRNS(png_structrp png_ptr, png_inforp info_ptr,
1177	1181	png_free(png_ptr, png_ptr->trans_alpha);
1178	1182	png_ptr->trans_alpha = png_voidcast(png_bytep,
1179	1183	png_malloc(png_ptr, PNG_MAX_PALETTE_LENGTH));
1184	+	memset(png_ptr->trans_alpha, 0xff, PNG_MAX_PALETTE_LENGTH);
1180	1185	memcpy(png_ptr->trans_alpha, trans_alpha, (size_t)num_trans);
1181	1186	}
1182	1187	else
		

Comments 0



Please [sign in](#) to comment.