New issue

Jump to bottom

A USE AFTER FREE BUG #863

Closed **ash1852** opened this issue on Jun 17 · 3 comments

ash1852 commented on Jun 17

Hi, I found a potential memory leak bug in the project source code of libsdl, I have shown the execution sequence of the program that may generate the bug on a diagram which is shown below.
The text in red illustrates the steps that generate the bug
The red arrows represent call relationships
The green text illustrates the files and functions whose code snippets are located below the green text.

the code snippet related to libsdl of this bug is shown below:

SDL-1.2/src/video/x11/SDL_x11yuv.c
Lines 375 to 381 in e1c3a1a

```
375     if ( hwdata->image != NULL && hwdata->image->pitches[0] != (width*bpp) ) {
376             /* Ajust overlay width according to pitch */
377             XFree(hwdata->image);
378             width = hwdata->image->pitches[0] / bpp;
379             hwdata->image = SDL_NAME(XvCreateImage)(GFX_Display, xv_port, format,
380                                                     0, width, height);
381     }
```

I look forward to your reply and thank you very much for your patience!

sezero commented on Jun 17 Collaborator

Fix would simply be moving XFree() a line below: **@icculus**, **@slouken**?

```
diff --git a/src/video/x11/SDL_x11yuv.c b/src/video/x11/SDL_x11yuv.c
index 62698df..0d5754e 100644
--- a/src/video/x11/SDL_x11yuv.c
+++ b/src/video/x11/SDL_x11yuv.c
@@ -374,8 +374,8 @@ SDL_Overlay *X11_CreateYUVOverlay(_THIS, int width, int height, Uint32 format, S
 #ifdef PITCH_WORKAROUND
                if ( hwdata->image != NULL && hwdata->image->pitches[0] != (width*bpp) ) {
                        /* Ajust overlay width according to pitch */
-                       XFree(hwdata->image);
                        width = hwdata->image->pitches[0] / bpp;
+                       XFree(hwdata->image);
                        hwdata->image = SDL_NAME(XvCreateImage)(GFX_Display, xv_port, format,
                                                                0, width, height);
                }
```

slouken commented on Jun 18 — Collaborator

Yep, go ahead and fix it.

sezero closed this as completed in d7e0020 on Jun 18

---

smcv commented on Aug 1

CVE-2022-34568 has apparently been assigned to this.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

4 participants