Doomsday Engine - Bug #870

possible index-out-of-bounds? (dgl_texture.c)

2010-03-03 23:36 - arclore

Status:	Closed	**Start date:**	2010-03-03
Priority:	Normal	**% Done:**	100%
Assignee:	danij		
Category:			
Target version:	1.9.0-beta6		

Description

From line 399:
void GL_GetColorPaletteRGB(DGLuint id, DGLubyte rgb[3], ushort idx) {
if(id != 0 && id - 1 < numColorPalettes) {
const gl_colorpalette_t* pal = &colorPalettes[id-1];

```
if(idx >= pal->num)
            VERBOSE(
            Con_Message("GL_GetColorPaletteRGB: Warning, color idx %u "
                        "out of range in palette %u.\n", idx, id))

idx = MINMAX_OF(0, idx, pal->num) * 3;
        rgb[CR] = pal->data[idx];
        rgb[CG] = pal->data[idx + 1];
        rgb[CB] = pal->data[idx + 2];
    }
}
elsewhere:
#define MINMAX_OF(a, x, b)  ((x) < (a)? (a) : (x) > (b)? (b) : (x))
```

The ConMessage says that an idx equal to or greater than pal->num is invalid. But the MINMAX_OF macro limits idx to pal->num, INCLUSIVE.
Say pal->num is 5. Based on the code, that means pal->num is [15]. If you pass an idx of 6 to the function, it tells you that it's out of range. But then it goes right ahead and tries to get pal->data[15], pal->data[16] and pal->data[17] anyway. Perhaps it should be MINMAX_OF(0, idx, (pal->num - 1)) * 3 instead?

Labels: OpenGL Renderer

History

#1 - 2012-12-19 09:50 - danij

Fixed for 1.9.0-beta6.9