ZAngband Bugs

Brought to you by: antimatter, rr9, sfuerst

#671 integer underflow bug

Milestone: Borg **Status:** open **Owner:** nobody **Labels:** None
Priority: 5
Updated: 2021-08-30 **Created:** 2021-08-30 **Creator:** Bjong Ho Son **Private:** No

in src/tk/plat.c, the variable `fileheader.bfOffBits` is tainted so that `ncol` can be overflowed. Then it is used as an argument to memory allocation function.

```
    /* Read the "BITMAPFILEHEADER" */
    rd_u16b(f, &(fileheader.bfType));
    rd_u32b(f, &(fileheader.bfSize));
    rd_u16b(f, &(fileheader.bfReserved1));
    rd_u16b(f, &(fileheader.bfReserved2));
    rd_u32b(f, &(fileheader.bfOffBits));

    /* Read the "BITMAPINFOHEADER" */
    rd_u32b(f, &(infoheader.biSize));
    rd_u32b(f, &(infoheader.biWidth));
    rd_u32b(f, &(infoheader.biHeight));
    rd_u16b(f, &(infoheader.biPlanes));
    rd_u16b(f, &(infoheader.biBitCount));
    rd_u32b(f, &(infoheader.biCompresion));
    rd_u32b(f, &(infoheader.biSizeImage));
    rd_u32b(f, &(infoheader.biXPelsPerMeter));
    rd_u32b(f, &(infoheader.biYPelsPerMeter));
    rd_u32b(f, &(infoheader.biClrUsed));
    rd_u32b(f, &(infoheader.biClrImportand));

    /* Verify the header */
    if (feof(f) ||
        (fileheader.bfType != 19778) ||
        (infoheader.biSize != 40))
    {
        quit_fmt("Incorrect BMP file format %s", Name);
    }

    /* The two headers above occupy 54 bytes total */
    /* The "bfOffBits" field says where the data starts */
    /* The "biClrUsed" field does not seem to be reliable */
    /* Compute number of colors recorded */
    ncol = (fileheader.bfOffBits - 54) / 4;


    if (ncol)
    {
        /* Create palette */
        C_MAKE(pal, ncol * 3, byte);
    }
```

Discussion

Bjong Ho Son - *2021-08-30*

sorry, "ncol can be overflowed" was a typo. I meant underflowed.

Last edit: Bjong Ho Son 2021-08-30

Log in to post a comment.

San Diego, CA 92101
+1 (858) 454-5900

Resources

Support

Site Documentation

Site Status

Terms Privacy Opt Out Advertise