TALOS-2026-2358

LibRaw x3f_thumb_loader heap-based buffer overflow vulnerability

APRIL 7, 2026

CVE NUMBER

SUMMARY

CONFIRMED VULNERABLE VERSIONS

PRODUCT URLS

CVSSV3 SCORE

CWE

DETAILS

LibRaw::x3f_thumb_loader() src/x3f/x3f_parse_process.cpp

```
void LibRaw::x3f_thumb_loader()
{
    [...]

    x3f_directory_entry_header_t *DEH = &DE->header;
    x3f_image_data_t *ID = &DEH->data_subsection.image_data;

    [...]

    else if (imgdata.thumbnail.tformat == LIBRAW_THUMBNAIL_BITMAP)
    {
[1]     imgdata.thumbnail.tlength = ID->columns * ID->rows * 3;
[2]     imgdata.thumbnail.thumb = (char *)malloc(ID->columns * ID->rows * 3);
        char *src0 = (char *)ID->data;
        for (int row = 0; row < (int)ID->rows; row++)
        {
[3]         int offset = row * ID->row_stride;
[4]         if (offset + ID->columns * 3 > ID->data_size)
                break;
[5]         char *dest = &imgdata.thumbnail.thumb[row * ID->columns * 3];
            char *src = &src0[offset];
[6]         memmove(dest, src, ID->columns * 3);
        }
    }

    [...]
}
```

ID->columns ID->rows ID->row_stride

uint32_t x3f_image_data_t

[1] [2] columns * rows * 3

uint32_t

UINT32_MAX malloc()

[2] malloc()

rows [5] row * columns * 3 [6] memmove()

columns = 50000 rows = 30000 50000 * 30000 * 3 = 4,500,000,000 4,500,000,000 mod 2^32 = 205,032,704

malloc()

[4]

row_stride row_stride = 1

unpack_thumb()

-DUSE_X3FTOOLS

TIMELINE

CREDIT

VULNERABILITY REPORTS NEXT REPORT PREVIOUS REPORT

TALOS-2026-2359 TALOS-2026-2331

© 2026 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy.