New issue

Jump to bottom

bugs found by our bug scanner #194

Closed lqiulin opened this issue on Feb 18, 2019 · 4 comments

lqiulin commented on Feb 18, 2019

Hi all,

Our bug scanner has reported some bugs.
Bug triggering files are attached.

Bug-1:div/mod-zero

1. in function `cp_create` ,jpc_enc.c#749
   `if (jpc_fixtodbl(tcp->ilyrrates[lyrno]) > ((double) cp->totalsize)/ cp->rawsize) { jas_eprintf("warning: intermediate layer rates must be less than overall rate\n"); goto error; }`
   Divisor: rawsize
   Result: Could be 0, Please Check.

2. in function `jjpc_dec_tileinit` , jpc_dec.c#736~#738
   `if (!(tcomp->data = jas_seq2d_create(JPC_CEILDIV(tile->xstart, cmpt->hstep), JPC_CEILDIV(tile->ystart, cmpt->vstep), JPC_CEILDIV(tile->xend, cmpt->hstep), JPC_CEILDIV(tile->yend, cmpt->vstep)))) { return -1; }`
   Divisor: cmpt->hstep, cmpt->vstep
   Result: Could be 0, Please Check.

3.in function `jpc_dec_process_siz` , jpc_dec.c#1270~#1273,#1339~#1342
`if (!(tcomp->data = jas_seq2d_create(JPC_CEILDIV(tile->xstart, cmpt->hstep), JPC_CEILDIV(tile->ystart, cmpt->vstep), JPC_CEILDIV(tile->xend, cmpt->hstep), JPC_CEILDIV(tile->yend, cmpt->vstep)))) { return -1; }`
`cmpt->width = JPC_CEILDIV(dec->xend, cmpt->hstep) - JPC_CEILDIV(dec->xstart, cmpt->hstep); cmpt->height = JPC_CEILDIV(dec->yend, cmpt->vstep) - JPC_CEILDIV(dec->ystart, cmpt->vstep);`
`tcomp->xstart = JPC_CEILDIV(tile->xstart, cmpt->hstep); tcomp->ystart = JPC_CEILDIV(tile->ystart, cmpt->vstep); tcomp->xend = JPC_CEILDIV(tile->xend, cmpt->hstep); tcomp->yend = JPC_CEILDIV(tile->yend, cmpt->vstep);`
Divisor: cmpt->hstep, cmpt->vstep
Result: Could be 0, Please Check.

4.in function `jas_cmxform_apply` , jas_cm.c#542
`*bufptr = (v - bias) / scale;`
Divisor: scale
Result: Could be 0, Please Check.

kloczek commented on Mar 9, 2019

Can you tell something about your scanner? :)
Is it possible to have look on it or try it?

stuartly commented on May 17, 2019

Sure, the link of the scanner is: https://github.com/stuartly/MissingCheck

MaxKellermann commented on Jun 30, 2020 Contributor

Bug 1 has been fixed in our fork: https://github.com/jasper-maint/jasper/

jubalh closed this as completed in fd564ee on Jul 28, 2020

jubalh added a commit to jubalh/buildroot that referenced this issue on Jul 28, 2020

`Update Jasper to 2.0.19` ... `3c4f2bc`

abergmann commented on Jul 19, 2021

CVE-2021-27845 was assigned to this issue.

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development

No branches or pull requests

5 participants