Name – Yolando Pereira
ypereira@andrew.cmu.edu

1.

jas_image_create
/home/tim/jasper-1.900.1-analyze/src/libjasper/base/jas_image.c:159
0x804a540 Signed integer overflow in multiplication
0x804a55a Signed integer overflow in multiplication
0x804a578 Unsigned integer overflow in addition
TP, INT30 - C. Calculation of rawsize from height and width may wrap
INT32 - C. Multiplication operation of Signed integers cmptparm->width, cmptparm->height and cmptparm->prec may overflow

2.

jas_image_cmpt_create
/home/tim/jasper-1.900.1-analyze/src/libjasper/base/jas_image.c:321
0x804aaec Signed integer overflow in multiplication
INT32 - C. Multiplication operation of Signed integers cmpt->width_, cmpt->height_ and cmpt->cps_ may overflow

3.

jas_stream_ungetc
/home/tim/jasper-1.900.1-analyze/src/libjasper/base/jas_stream.c:503
0x8052063 Truncation
INT31 - C. Unsigned Character stream->ptr_ takes its value from signed int c, may result in lost data.

4.

jas_stream_read
/home/tim/jasper-1.900.1-analyze/src/libjasper/base/jas_stream.c:520
0x805215a Truncation
INT31 - C. Unsigned Character bufptr takes its value from signed int c, may result in lost data.

5.

jas_stream_tell
/home/tim/jasper-1.900.1-analyze/src/libjasper/base/jas_stream.c:689
0x80529c2 Unsigned integer overflow in addition
INT32 - C Addition of signed integers offset and adjust may result in overflow of returned value. Depending on implementation long may be 32-bit.

6.

jp2_validate
/home/tim/jasper-1.900.1-analyze/src/libjasper/jp2/jp2_dec.c:467
0x805c4df Signed integer overflow in left-shift
INT34 – C. Attempting to shift char type by more bits than exist in the operand

7.

jp2_box_get
/home/tim/jasper-1.900.1-analyze/src/libjasper/jp2/jp2_cod.c:272
0x805ca1f Unsigned integer overflow in subtraction
INT 30 – C. Subraction of box->len and JP2_BOX_HDRLEN(false) may result in unsigned integer wrapping

8.

jpc_dec_process_siz
/home/tim/jasper-1.900.1-analyze/src/libjasper/jpc/jpc_dec.c:1194
0x8078e1e Unsigned integer overflow in subtraction
INT 30 – C. Subraction of JPC_CEILDIV(dec->xend, cmpt->hstep) - JPC_CEILDIV(dec->xstart, cmpt->hstep) may result in wrapping

9.

jpc_dec_process_siz
/home/tim/jasper-1.900.1-analyze/src/libjasper/jpc/jpc_dec.c:1196
0x8078e99 Unsigned integer overflow in subtraction
INT 30 – C. Subraction of JPC_CEILDIV(dec->yend, cmpt->vstep) - JPC_CEILDIV(dec->ystart, cmpt->vstep) may result in wrapping

10.

jpc_dec_process_siz
/home/tim/jasper-1.900.1-analyze/src/libjasper/jpc/jpc_dec.c:1204
0x8078eef Unsigned integer overflow in subtraction
0x8078efe Unsigned integer overflow in addition
INT 31 – C. dec->numhtiles = JPC_CEILDIV(dec->xend - dec->tilexoff, dec->tilewidth) attempts to store unsigned integer in a signed integer
INT 30 – C. dec->xend - dec->tilexoff may result in unsigned wrapping

11.

jpc_dec_process_siz
/home/tim/jasper-1.900.1-analyze/src/libjasper/jpc/jpc_dec.c:1205
0x8078f3a Unsigned integer overflow in subtraction
INT 31 – C. dec->numvtiles = JPC_CEILDIV(dec->yend - dec->tileyoff, dec->tileheight) attempts to store unsigned integer in a signed integer
INT 30 – C. dec->yend - dec->tileyoff may result in unsigned wrapping

12.

jpc_dec_process_siz
/home/tim/jasper-1.900.1-analyze/src/libjasper/jpc/jpc_dec.c:1206
0x8078f86 Signed integer overflow in multiplication
INT 32 – C. dec->numtiles = dec->numhtiles * dec->numvtiles may result in signed overflow

13.

jpc_dec_process_siz
/home/tim/jasper-1.900.1-analyze/src/libjasper/jpc/jpc_dec.c:1217
0x807903e Unsigned integer overflow in multiplication
INT 30 – C. dec->tileyoff + vtileno * dec->tileheight would result in unsigned integer wrapping

14.

jpc_dec_process_siz
/home/tim/jasper-1.900.1-analyze/src/libjasper/jpc/jpc_dec.c:1219
0x8079074 Unsigned integer overflow in multiplication
INT 30 – C. dec->tileyoff + vtileno * dec->tileheight would result in unsigned integer wrapping

15.

jpc_dec_process_siz
/home/tim/jasper-1.900.1-analyze/src/libjasper/jpc/jpc_dec.c:1221
0x80790b6 Unsigned integer overflow in multiplication
0x80790bf Unsigned integer overflow in addition
INT 30 – C. dec->tilexoff + (htileno + 1) * dec->tilewidth would result in unsigned integer wrapping

16.

jpc_dec_process_siz
/home/tim/jasper-1.900.1-analyze/src/libjasper/jpc/jpc_dec.c:1223
0x80790f8 Unsigned integer overflow in multiplication
0x8079101 Unsigned integer overflow in addition
INT 30 – C. dec->tileyoff + (vtileno + 1) * dec->tileheight would result in unsigned integer wrapping

17.

jas_matrix_create
/home/tim/jasper-1.900.1-analyze/src/libjasper/base/jas_seq.c:114
0x8086302 Signed integer overflow in multiplication
INT 32 – C. Multiplication between signed integers numrows and numcols may result in overflow