**Vulnerability Disclosure – Jbig2dec library (latest version)**

**Title:** Denial of Service (crash) due to access Null pointer when parsing an illegal file.

**Vendor:** Open Source (<https://artifex.com/developers-ghostscript-jbig2dec/> )

**Affected Product name(s) and versions:** Jbig2dec latest version including stable version (0.13)

**Platform used (OS):** Linux – Ubuntu 16.04 x86\_64

**Summary of the issue:**

Jbig2dec latest version, as used in MuPDF and Ghostscript, has a NULL pointer dereference in the jbig2\_huffman\_get function in jbig2\_huffman.c. For example, the jbig2dec utility will crash (segmentation fault) when parsing an invalid file.

**Example output:**

./jbig2dec ../crash/crash0000

jbig2dec FATAL ERROR missing glyph 0/0! (segment 0x01)

ASAN:DEADLYSIGNAL

=================================================================

==79982==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7fc274de397d bp 0x7ffefb069590 sp 0x7ffefb069370 T0)

#0 0x7fc274de397c (/home/root/fuzz/jbig2dec-clang/.libs/libjbig2dec.so.0+0x1697c)

#1 0x7fc274dfc925 (/home/root/fuzz/jbig2dec-clang/.libs/libjbig2dec.so.0+0x2f925)

#2 0x7fc274df404d (/home/root/fuzz/jbig2dec-clang/.libs/libjbig2dec.so.0+0x2704d)

#3 0x7fc274deff04 (/home/root/fuzz/jbig2dec-clang/.libs/libjbig2dec.so.0+0x22f04)

#4 0x7fc274de8a2e (/home/root/fuzz/jbig2dec-clang/.libs/libjbig2dec.so.0+0x1ba2e)

#5 0x7fc274dde0a0 (/home/root/fuzz/jbig2dec-clang/.libs/libjbig2dec.so.0+0x110a0)

#6 0x4eaea2 (/home/root/fuzz/jbig2dec-clang/.libs/lt-jbig2dec+0x4eaea2)

#7 0x7fc273a9d82f (/lib/x86\_64-linux-gnu/libc.so.6+0x2082f)

#8 0x418fe8 (/home/root/fuzz/jbig2dec-clang/.libs/lt-jbig2dec+0x418fe8)

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV (/home/root/fuzz/jbig2dec-clang/.libs/libjbig2dec.so.0+0x1697c)

==79982==ABORTING

**Debug info:**

Starting program: /home/root/fuzz/jbig2dec/jbig2dec ../crash/crash0000

jbig2dec FATAL ERROR missing glyph 0/0! (segment 0x01)

Program received signal SIGSEGV, Segmentation fault.

jbig2\_huffman\_get (hs=hs@entry=0x651370, table=0x0, oob=oob@entry=0x7fffffffc970) at jbig2\_huffman.c:274

274 int log\_table\_size = table->log\_table\_size;

(gdb) p table

$1 = (const Jbig2HuffmanTable \*) 0x0

(gdb) bt

#0 jbig2\_huffman\_get (hs=hs@entry=0x651370, table=0x0, oob=oob@entry=0x7fffffffc970) at jbig2\_huffman.c:274

#1 0x0000000000408092 in jbig2\_decode\_text\_region (ctx=ctx@entry=0x619240, segment=segment@entry=0x626da0, params=params@entry=0x627120, dicts=dicts@entry=0x626fd0, n\_dicts=n\_dicts@entry=1,

image=image@entry=0x651320, data=0x61a474 "\336\177\001", size=34, GR\_stats=0x64f2c0 "", as=0x626e00, ws=0x626de0) at jbig2\_text.c:340

#2 0x0000000000405e87 in jbig2\_decode\_symbol\_dict (GR\_stats=<optimized out>, GB\_stats=<optimized out>, size=<optimized out>, data=<optimized out>, params=0x7fffffffcce0, segment=0x626da0, ctx=0x619240)

at jbig2\_symbol\_dict.c:496

#3 jbig2\_symbol\_dictionary (ctx=ctx@entry=0x619240, segment=segment@entry=0x626da0, segment\_data=<optimized out>) at jbig2\_symbol\_dict.c:996

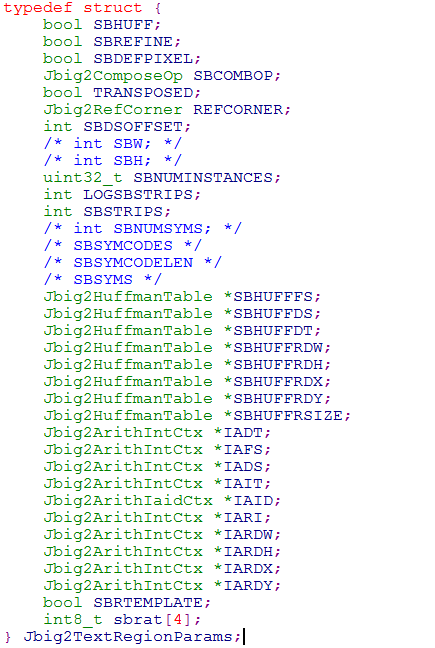
#4 0x0000000000404530 in jbig2\_parse\_segment (ctx=ctx@entry=0x619240, segment=segment@entry=0x626da0, segment\_data=<optimized out>) at jbig2\_segment.c:234

#5 0x0000000000403a21 in jbig2\_data\_in (ctx=ctx@entry=0x619240, data=data@entry=0x7fffffffce60 "\227JB2\r\n\032\n\001", size=<optimized out>) at jbig2.c:312

#6 0x0000000000401697 in main (argc=<optimized out>, argv=0x7fffffffdf88) at jbig2dec.c:456

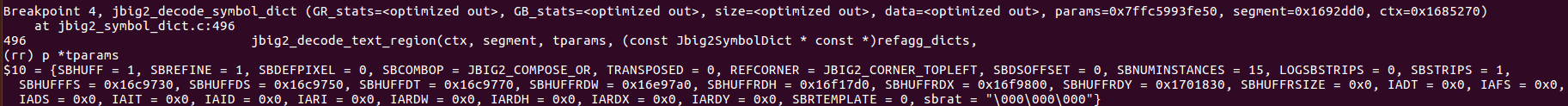
**Explanation:**

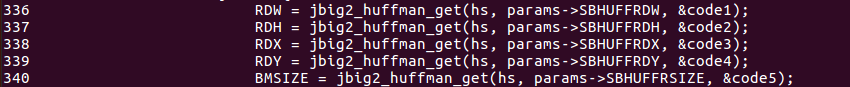
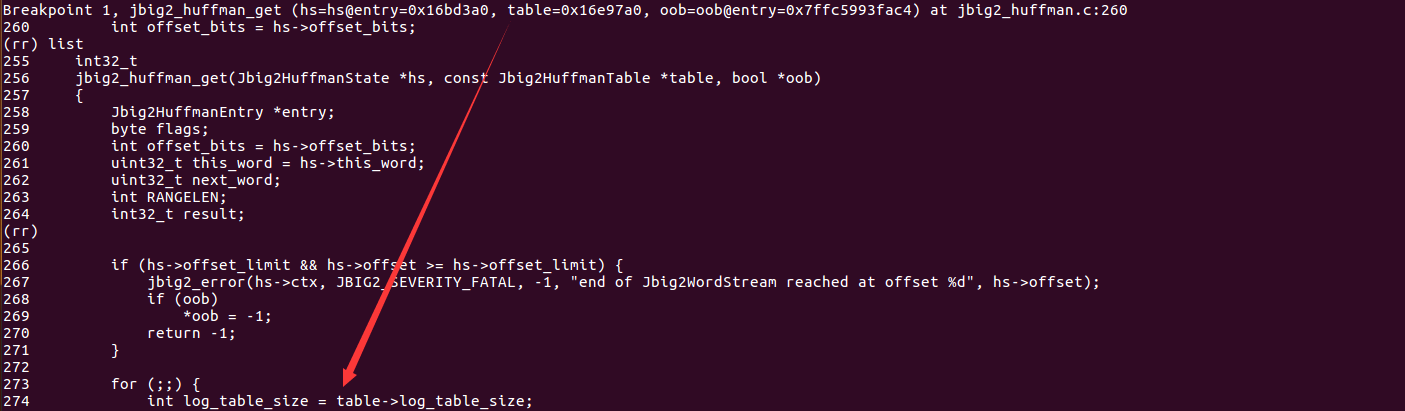
Object tparams is the instance of struct Jbig2TextRegionParams.

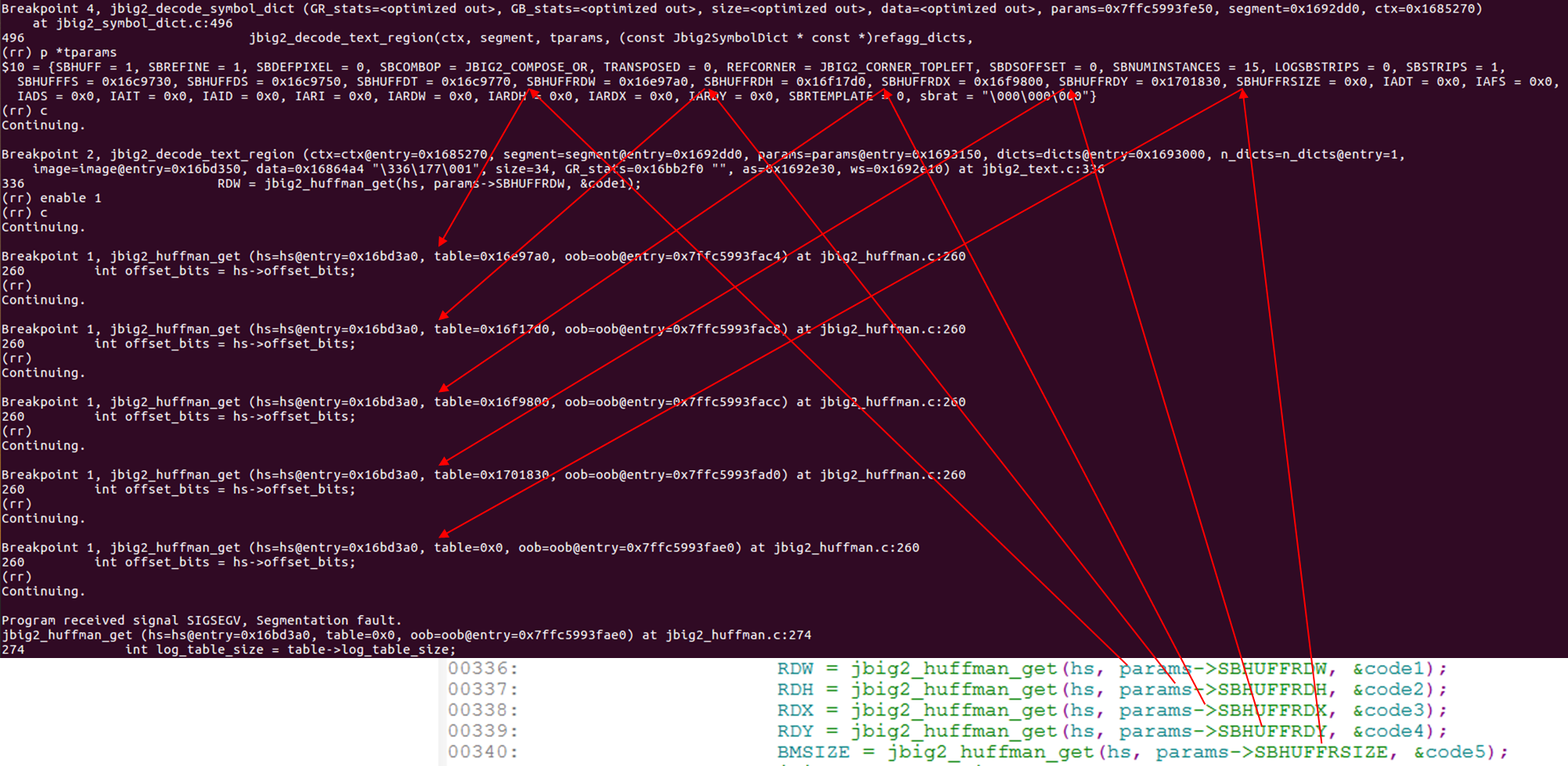


tparams instance is initialized in line 449 of jbig2\_decode\_symbol\_dict function in jbig2\_symbol\_dict.c. And, it is passed into jbig2\_decode\_text\_region as a parameter in line 496 of jbig2\_decode\_symbol\_dict function. We can see that, tparms->SBHUFFRSIZE is not changed from line 449 to line 496.





In line 340 of jbig2\_test.c, tparams-> SBHUFFRSIZE is passed to jbig2\_huffman\_get function as a parameter. Then when program try to access tparams-> SBHUFFRSIZE->log\_table\_size, it crash for Null pointer deference.



**Suggestion for patch:**

Assign tparams-> SBHUFFRSIZE with something instead 0x0.

**Credits:**

Young\_X and Chenghao Rong from VARAS@IIE