New issue

Jump to bottom

heap-buffer-overflow in base64_encode #63

Open **Cvjark** opened this issue on Jul 11 · 0 comments

Cvjark commented on Jul 11

sample file

id11_heap-buffer-overflow_base64_encode.zip

command to reproduce

```
./swfmill swf2xml [sample file] /dev/null
```

crash detail

```
==55556==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000019813 at pc
0x0000005311c9 bp 0x7ffedbddc7f0 sp 0x7ffedbddc7e8
WRITE of size 1 at 0x602000019813 thread T0
    #0 0x5311c8 in base64_encode /home/bupt/Desktop/swfmill/src/base64.c:46:10
    #1 0x5d5152 in SWF::UnknownTag::writeXML(_xmlNode*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriteXML.cpp:3881:12
    #2 0x5bc1ee in SWF::Header::writeXML(_xmlNode*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriteXML.cpp:375:11
    #3 0x53e1d2 in SWF::File::getXML(SWF::Context*)
/home/bupt/Desktop/swfmill/src/SWFFile.cpp:215:11
    #4 0x53e4f0 in SWF::File::saveXML(_IO_FILE*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/SWFFile.cpp:239:19
    #5 0x54eebe in swfmill_swf2xml(int, char**) /home/bupt/Desktop/swfmill/src/swfmill.cpp:147:24
    #6 0x7f93171f1c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #7 0x4224d9 in _start (/home/bupt/Desktop/swfmill/src/swfmill+0x4224d9)

0x602000019813 is located 0 bytes to the right of 3-byte region [0x602000019810,0x602000019813)
allocated by thread T0 here:
    #0 0x4fa7c8 in operator new[](unsigned long) /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_new_delete.cpp:102
    #1 0x5d5140 in SWF::UnknownTag::writeXML(_xmlNode*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriteXML.cpp:3879:19
    #2 0x5bc1ee in SWF::Header::writeXML(_xmlNode*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriteXML.cpp:375:11
```

```
    #3 0x53e1d2 in SWF::File::getXML(SWF::Context*)
/home/bupt/Desktop/swfmill/src/SWFFile.cpp:215:11
    #4 0x53e4f0 in SWF::File::saveXML(_IO_FILE*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/SWFFile.cpp:239:19
    #5 0x54eebe in swfmill_swf2xml(int, char**) /home/bupt/Desktop/swfmill/src/swfmill.cpp:147:24
    #6 0x7f93171f1c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/swfmill/src/base64.c:46:10 in
base64_encode
Shadow bytes around the buggy address:
  0x0c047fffb2b0: fa fa 02 fa fa fa 07 fa fa fa 02 fa fa fa 05 fa
  0x0c047fffb2c0: fa fa 02 fa fa fa 00 01 fa fa 04 fa fa fa 05 fa
  0x0c047fffb2d0: fa fa 00 03 fa fa 07 fa fa fa 00 01 fa fa 06 fa
  0x0c047fffb2e0: fa fa 07 fa fa fa 04 fa fa fa 06 fa fa fa 06 fa
  0x0c047fffb2f0: fa fa 07 fa fa fa 05 fa fa fa 05 fa fa fa 00 03
=>0x0c047fffb300: fa fa[03]fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fffb310: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fffb320: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fffb330: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fffb340: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fffb350: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==55556==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant