New issue

Jump to bottom

issue about memory allocation #65

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

Cvjark commented on Jul 11 • edited

sample file

id0_allocation-size-too-big_new.zip

command to reproduce

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

crash detail

```
==55540==ERROR: AddressSanitizer: requested allocation size 0xfffffffffffff4d6 (0x4d8 after
adjustments for alignment, red zones etc.) exceeds maximum supported size of 0x10000000000 (thread
T0)
    #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 0x68bef0 in SWF::UnknownOpCode::parse(SWF::Reader*, int, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFParser.cpp:12214:10

==55540==HINT: if you don't care about these errors you may set allocator_may_return_null=1
SUMMARY: AddressSanitizer: allocation-size-too-big /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_new_delete.cpp:102 in operator new[](unsigned long)
==55540==ABORTING
```

sample file

id14_alloc-dealloc-mismatch_delete.zip

command to reproduce

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

crash detail

```
==55572==ERROR: AddressSanitizer: alloc-dealloc-mismatch (operator new [] vs operator delete) on
0x6060000006e0
    #0 0x4fb060 in operator delete(void*) /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_new_delete.cpp:160
    #1 0x5d5223 in SWF::UnknownTag::writeXML(_xmlNode*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriteXML.cpp:3886:4
    #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 0x7f7a73af4c86 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)

0x6060000006e0 is located 0 bytes inside of 57-byte region [0x6060000006e0,0x606000000719)
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 0x7f7a73af4c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310

SUMMARY: AddressSanitizer: alloc-dealloc-mismatch /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_new_delete.cpp:160 in operator delete(void*)
==55572==HINT: if you don't care about these errors you may set
ASAN_OPTIONS=alloc_dealloc_mismatch=0
==55572==ABORTING
```

  **Cvjark** changed the title ~~**allocation-size-too-big**~~ **issue about memory allocation** on Jul 11

Assignees

No one assigned

Labels

None yet

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant