New issue

Jump to bottom

Stack-overflow occurred in operator new(unsigned long) of pyc_object.cpp. #291

Open **yangfar** opened this issue on Oct 17 · 0 comments

yangfar commented on Oct 17

Version Info

Pycdc latest commit https://github.com/zrax/pycdc/commit/44a730f3a889503014fec94ae6e62d8401cb75e5

Command

./pycdas ./POC

Crash output

AddressSanitizer:DEADLYSIGNAL

==2840==ERROR: AddressSanitizer: stack-overflow on address 0x7fff4f412fd8 (pc 0x0000004bb791 bp 0x000000587730 sp 0x7fff4f412fd0 T0)
#0 0x4bb791 in __sanitizer::StackDepotBase<__sanitizer::StackDepotNode, 1, 20>::Put(__sanitizer::StackTrace, bool*) (/home/hjsz/fuzz_software/pycdc/build/pycdas+0x4bb791)
#1 0x4bb766 in __sanitizer::StackDepotPut(__sanitizer::StackTrace) (/home/hjsz/fuzz_software/pycdc/build/pycdas+0x4bb766)
#2 0x4247e9 in __asan::Allocator::Allocate(unsigned long, unsigned long, __sanitizer::BufferedStackTrace*, __asan::AllocType, bool) (/home/hjsz/fuzz_software/pycdc/build/pycdas+0x4247e9)
#3 0x425079 in __asan::asan_memalign(unsigned long, unsigned long, __sanitizer::BufferedStackTrace*, __asan::AllocType) (/home/hjsz/fuzz_software/pycdc/build/pycdas+0x425079)
#4 0x4cacf2 in operator new(unsigned long) (/home/hjsz/fuzz_software/pycdc/build/pycdas+0x4cacf2)
#5 0x4feff2 in CreateObject(int) /home/hjsz/fuzz_software/pycdc/pyc_object.cpp:58:16
#6 0x50040a in LoadObject(PycData*, PycModule*) /home/hjsz/fuzz_software/pycdc/pyc_object.cpp:80:15
#7 0x504865 in PycDict::load(PycData*, PycModule*) /home/hjsz/fuzz_software/pycdc/pyc_sequence.cpp:84:15
#8 0x50080b in LoadObject(PycData*, PycModule*) /home/hjsz/fuzz_software/pycdc/pyc_object.cpp:84:18
#9 0x504865 in PycDict::load(PycData*, PycModule*) /home/hjsz/fuzz_software/pycdc/pyc_sequence.cpp:84:15
SUMMARY: AddressSanitizer: stack-overflow (/home/hjsz/fuzz_software/pycdc/build/pycdas+0x4bb791) in __sanitizer::StackDepotBase<__sanitizer::StackDepotNode, 1, 20>::Put(__sanitizer::StackTrace, bool*)
==2840==ABORTING

POC

POC.zip

Report of the Information Security Laboratory of Ocean University of China @OUC_ISLOUC @OUC_Blue_Whale

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant