EOSIO / eos Public archive

[heap-buffer-overflow] happens while using txn_test_gen_plugin #10820

Open **renardbebe** opened this issue on Oct 19, 2021 · 3 comments

Labels track-in-jira

renardbebe commented on Oct 19, 2021

EOS: 2.1.0
Ubuntu: 20.04
Compiler: llvm-7 clang-7 clang++-7 llvm-cov-7

I want to use `txn_test_gen_plugin` to generate transactions, and the process is following the guidance: https://github.com/EOSIO/eos/blob/develop/plugins/txn_test_gen_plugin/README.md

I have started the producer node (`eosio`) and non-producer node (`bp.a`), and deployed the bios contract.

```
$ cleos set contract eosio /root/eos-2.1.0/eos/build/contracts/contracts/eosio.bios/
eosio.bios.wasm eosio.bios.abi
```

Then, when I use the command to initialize the accounts txn_test_gen_plugin uses, **heap-buffer-overflow** happens:

```
$ curl --data-binary '["eosio", "5KQwrPbwdL6PhXujxW37FSSQZ1JiwsST4cqQzDeyXtP79zkvFD3"]'
http://127.0.0.1:8888/v1/txn_test_gen/create_test_accounts
```

Logs of eosio node:

```
info  2021-10-19T05:30:57.402 nodeos    producer_plugin.cpp:2333      produce_block        ]
Produced block aa368708758ed956... #61 @ 2021-10-19T05:30:57.500 signed by eosio [trxs: 0, lib:
60, confirmed: 0]
info  2021-10-19T05:30:57.594 net-0     net_plugin.cpp:3433           connection_monitor   ] p2p
client connections: 1/25, peer connections: 0/0
```

```
info  2021-10-19T05:30:57.902 nodeos    producer_plugin.cpp:2333      produce_block        ]
Produced block eb95e9e4d0d8906e... #62 @ 2021-10-19T05:30:58.000 signed by eosio [trxs: 0, lib:
61, confirmed: 0]
info  2021-10-19T05:30:58.401 nodeos    producer_plugin.cpp:2333      produce_block        ]
Produced block a8db3c032b2ac8f6... #63 @ 2021-10-19T05:30:58.500 signed by eosio [trxs: 0, lib:
62, confirmed: 0]
info  2021-10-19T05:30:58.901 nodeos    producer_plugin.cpp:2333      produce_block        ]
Produced block 473c9b09d2c56f34... #64 @ 2021-10-19T05:30:59.000 signed by eosio [trxs: 0, lib:
63, confirmed: 0]
info  2021-10-19T05:30:59.301 nodeos    producer_plugin.cpp:2333      produce_block        ]
Produced block 91d3cccbd891aeac... #65 @ 2021-10-19T05:30:59.500 signed by eosio [trxs: 0, lib:
64, confirmed: 0]
info  2021-10-19T05:30:59.902 nodeos    producer_plugin.cpp:2333      produce_block        ]
Produced block ed28d25ae2dd6758... #66 @ 2021-10-19T05:31:00.000 signed by eosio [trxs: 0, lib:
65, confirmed: 0]
info  2021-10-19T05:31:00.401 nodeos    producer_plugin.cpp:2333      produce_block        ]
Produced block 6ba3e5c44047d20e... #67 @ 2021-10-19T05:31:00.500 signed by eosio [trxs: 0, lib:
66, confirmed: 0]
info  2021-10-19T05:31:00.901 nodeos    producer_plugin.cpp:2333      produce_block        ]
Produced block 4f3357d2c3d89b81... #68 @ 2021-10-19T05:31:01.000 signed by eosio [trxs: 0, lib:
67, confirmed: 0]
info  2021-10-19T05:31:01.401 nodeos    producer_plugin.cpp:2333      produce_block        ]
Produced block 9eab505535c4df89... #69 @ 2021-10-19T05:31:01.500 signed by eosio [trxs: 0, lib:
68, confirmed: 0]
info  2021-10-19T05:31:01.538 nodeos    txn_test_gen_plugin.cp:132    create_test_accounts ]
create_test_accounts
=================================================================
==108558==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62100005ee7c at pc
0x00000058d049 bp 0x7ffdf793a540 sp 0x7ffdf7939ce8
READ of size 4477 at 0x62100005ee7c thread T0
    #0 0x58d048 in strlen (/root/eos-2.1.0/eos/build/bin/nodeos+0x58d048)
    #1 0x668bcd in std::char_traits<char>::length(char const*) /usr/bin/../lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/char_traits.h:335:9
    #2 0x668bcd in std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char>
>::basic_string<std::allocator<char> >(char const*, std::allocator<char> const&)
/usr/bin/../lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/basic_string.h:527
    #3 0x15cf35c in
eosio::txn_test_gen_plugin_impl::create_test_accounts(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::function<void
(std::shared_ptr<fc::exception> const&)> const&) /root/eos-
2.1.0/eos/plugins/txn_test_gen_plugin/txn_test_gen_plugin.cpp:139:59
    #4 0x15b5962 in eosio::txn_test_gen_plugin::plugin_startup()::$_0::operator()
(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::function<void (int, std::optional<fc::variant>)>) /root/eos-
2.1.0/eos/plugins/txn_test_gen_plugin/txn_test_gen_plugin.cpp:457:7
    #5 0x15b5962 in std::_Function_handler<void (std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::function<void (int,
std::optional<fc::variant>)>),
eosio::txn_test_gen_plugin::plugin_startup()::$_0>::_M_invoke(std::_Any_data const&,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >&&,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >&&,
std::function<void (int, std::optional<fc::variant>)>&&) /usr/bin/../lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/std_function.h:300
```

```
    #6 0x214cb88 in std::function<void (std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >, std::function<void (int, std::optional<fc::variant>)>)>::operator()
(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::function<void (int, std::optional<fc::variant>)>) const /usr/bin/../lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/std_function.h:688:14
    #7 0x214cb88 in eosio::http_plugin_impl::make_app_thread_url_handler(int, std::function<void
(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::function<void (int, std::optional<fc::variant>)>)>,
std::shared_ptr<eosio::http_plugin_impl>)::'lambda'(std::shared_ptr<eosio::detail::abstract_conn>,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::function<void (int, std::optional<fc::variant>)>)::operator()
(std::shared_ptr<eosio::detail::abstract_conn>, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::function<void (int,
std::optional<fc::variant>)>) const::'lambda'()::operator()() /root/eos-
2.1.0/eos/plugins/http_plugin/http_plugin.cpp:554
    #8 0x6af84e in appbase::execution_priority_queue::execute_highest() /root/eos-
2.1.0/eos/libraries/appbase/include/appbase/execution_priority_queue.hpp:42:27
    #9 0x692435 in appbase::application::exec() /root/eos-
2.1.0/eos/libraries/appbase/application.cpp:423:27
    #10 0x65d736 in main /root/eos-2.1.0/eos/programs/nodeos/main.cpp:143:13
    #11 0x7fa8fe77e0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #12 0x579bfd in _start (/root/eos-2.1.0/eos/build/bin/nodeos+0x579bfd)

0x62100005ee7c is located 0 bytes to the right of 4476-byte region [0x62100005dd00,0x62100005ee7c)
allocated by thread T0 here:
    #0 0x650c82 in operator new(unsigned long) (/root/eos-2.1.0/eos/build/bin/nodeos+0x650c82)
    #1 0x7519de in __gnu_cxx::new_allocator<char>::allocate(unsigned long, void const*)
/usr/bin/../lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/ext/new_allocator.h:114:27
    #2 0x7519de in std::allocator_traits<std::allocator<char> >::allocate(std::allocator<char>&,
unsigned long) /usr/bin/../lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/alloc_traits.h:444
    #3 0x7519de in std::_Vector_base<char, std::allocator<char> >::_M_allocate(unsigned long)
/usr/bin/../lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/stl_vector.h:343
    #4 0x15cf2b0 in
eosio::txn_test_gen_plugin_impl::create_test_accounts(std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> > const&, std::function<void
(std::shared_ptr<fc::exception> const&)> const&) /root/eos-
2.1.0/eos/plugins/txn_test_gen_plugin/txn_test_gen_plugin.cpp:139:59
    #5 0x15b5962 in eosio::txn_test_gen_plugin::plugin_startup()::$_0::operator()
(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::function<void (int, std::optional<fc::variant>)>) /root/eos-
2.1.0/eos/plugins/txn_test_gen_plugin/txn_test_gen_plugin.cpp:457:7
    #6 0x15b5962 in std::_Function_handler<void (std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::function<void (int,
std::optional<fc::variant>)>),
eosio::txn_test_gen_plugin::plugin_startup()::$_0>::_M_invoke(std::_Any_data const&,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >&&,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >&&,
std::function<void (int, std::optional<fc::variant>)>&&) /usr/bin/../lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/std_function.h:300
    #7 0x214cb88 in std::function<void (std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >, std::__cxx11::basic_string<char, std::char_traits<char>,
std::allocator<char> >, std::function<void (int, std::optional<fc::variant>)>)>::operator()
(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::function<void (int, std::optional<fc::variant>)>) const /usr/bin/../lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/std_function.h:688:14
    #8 0x214cb88 in eosio::http_plugin_impl::make_app_thread_url_handler(int, std::function<void
(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::function<void (int, std::optional<fc::variant>)>)>,
std::shared_ptr<eosio::http_plugin_impl>)::'lambda'(std::shared_ptr<eosio::detail::abstract_conn>,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >,
std::function<void (int, std::optional<fc::variant>)>)::operator()
(std::shared_ptr<eosio::detail::abstract_conn>, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::__cxx11::basic_string<char,
std::char_traits<char>, std::allocator<char> >, std::function<void (int,
std::optional<fc::variant>)>) const::'lambda'()::operator()() /root/eos-
2.1.0/eos/plugins/http_plugin/http_plugin.cpp:554
    #9 0x6af84e in appbase::execution_priority_queue::execute_highest() /root/eos-
2.1.0/eos/libraries/appbase/include/appbase/execution_priority_queue.hpp:42:27
    #10 0x65d736 in main /root/eos-2.1.0/eos/programs/nodeos/main.cpp:143:13
    #11 0x7fa8fe77e0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/root/eos-2.1.0/eos/build/bin/nodeos+0x58d048) in
strlen
Shadow bytes around the buggy address:
  0x0c4280003d70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4280003d80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4280003d90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4280003da0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4280003db0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c4280003dc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[04]
  0x0c4280003dd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280003de0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280003df0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280003e00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4280003e10: 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
  ==108558==ABORTING
```

- The config.ini file of eosio node (producer):

```
http-server-address = 0.0.0.0:8888
p2p-listen-endpoint = 0.0.0.0:9800
allowed-connection = any
p2p-max-nodes-per-host = 100
signature-provider =
EOS6MRyAjQq8ud7hVNYcfnVPJqcVpscN5So8BhtHuGYqET5GDW5CV=KEY:5KQwrPbwdL6PhXujxW37FSSQZ1JiwsST4cqQzDeyXtP

producer-name = eosio
plugin = eosio::http_plugin
plugin = eosio::chain_api_plugin
plugin = eosio::producer_plugin
plugin = eosio::producer_api_plugin
plugin = eosio::net_api_plugin
enable-stale-production = true
plugin = eosio::txn_test_gen_plugin
```

- The config.ini file of non-producer node:

```
http-server-address = 0.0.0.0:8889
p2p-listen-endpoint = 0.0.0.0:9801
allowed-connection = any
p2p-peer-address = localhost:9800
p2p-max-nodes-per-host = 100
signature-provider = public_key=KEY:private_key
producer-name = bp.a
plugin = eosio::http_plugin
plugin = eosio::chain_api_plugin
plugin = eosio::producer_plugin
plugin = eosio::net_api_plugin
plugin = eosio::history_api_plugin
plugin = eosio::txn_test_gen_plugin
```

Is there a bug, or which of my steps is wrong?
Waiting for any answer and solutions, thank you very much!

renardbebe commented on Oct 25, 2021 Author

Dear authors, any response?

node.log

heifner commented on Oct 26, 2021 Contributor

Just looking at the stack trace and it is failing on reading the token contract abi file from disk. Looks like it assumes you built the software yourself. Are you running from an install?

renardbebe commented on Oct 27, 2021 Author

@heifner Thanks for the reply.

I have built EOSIO from the source, following the guidance:
https://developers.eos.io/manuals/eos/latest/install/build-from-source/manual-build/platforms/ubuntu-18.04.
And I have deployed the token contract on 127.0.0.1:8888, the steps are following the official doc:
https://developers.eos.io/welcome/latest/smart-contract-guides/deploy-issue-and-transfer-tokens. I have tested that the transfer function works well:

```
executed transaction: eedcc879e7647789ece0e77f597476b16610c6409e2b39beefe89a5583556978  128 bytes
895 us
#   eosio.token <= eosio.token::transfer        {"from":"bp.b","to":"bp.a","quantity":"5379.0000
SYS","memo":"m"}
#          bp.b <= eosio.token::transfer        {"from":"bp.b","to":"bp.a","quantity":"5379.0000
SYS","memo":"m"}
#          bp.a <= eosio.token::transfer        {"from":"bp.b","to":"bp.a","quantity":"5379.0000
SYS","memo":"m"}
warning: transaction executed locally, but may not be confirmed by the network yet         ]
```

So, where is the problem?

sanaraufx added the **track-in-jira** label on Oct 27, 2021

Assignees

No one assigned

Labels

track-in-jira

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants