# OpenRTM-aist (C++) - バグ #4270

## StateMachine.hでheap-use-after-free

2017/10/18 10:00 - kanehiro

| | | | |
|---|---|---|---|
| **ステータス:** | 新規 | **開始日:** | 2017/10/18 |
| **優先度:** | 通常 | **期日:** | |
| **担当者:** | n-ando | **進捗率:** | 0% |
| **カテゴリ:** | | **予定工数:** | 0.00時間 |
| **対象バージョン:** | | | |

**説明**

こちらでロボットのシミュレーションによるテストを走らせる際に、Address Sanitizerを有効にして走らせているのですが、時々以下のようにheap-use-after-freeを検出します。
何かわかりますでしょうか。
なおソースはRELENG_1_1のものです。

```
04:53:18 =================================================================
04:53:18 ==20889==ERROR: AddressSanitizer: heap-use-after-free on address 0x6060003d6d10 at pc 0x7ffb31448be9 bp
fb41d7f6e0 sp 0x7ffb41d7f6d0
04:53:18 READ of size 8 at 0x6060003d6d10 thread T12
04:53:18 #0 0x7ffb31448be8 in RTC_Utils::StateMachine<RTC::LifeCycleState, RTC::PeriodicExecutionContext::DFPBase, R
Utils::StateHolder<RTC::LifeCycleState>, void (RTC::PeriodicExecutionContext::DFPBase::*)(RTC_Utils::StateHolder<RTC::LifeCycleStat
e> const&)>::worker() /home/jenkinshrg/openrtp/include/openrtm-1.1/rtm/StateMachine.h:698
04:53:18 #1 0x7ffb31448be8 in RTC::PeriodicExecutionContext::DFPBase::worker() /home/jenkinshrg/openrtp/include/op
tm-1.1/rtm/PeriodicExecutionContext.h:978
04:53:18 #2 0x7ffb31448be8 in RTC::PeriodicExecutionContext::invoke_worker::operator()(RTC::PeriodicExecutionContext::C
mp&) /home/jenkinshrg/openrtp/include/openrtm-1.1/rtm/PeriodicExecutionContext.h:1467
04:53:18 #3 0x7ffb31448be8 in RTC::PeriodicExecutionContext::invoke_worker std::for_each<__gnu_cxx::__normal_iterato
TC::PeriodicExecutionContext::Comp*, std::vector<RTC::PeriodicExecutionContext::Comp, std::allocator<RTC::PeriodicExecutionConte
xt::Comp> > >, RTC::PeriodicExecutionContext::invoke_worker>(__gnu_cxx::__normal_iterator<RTC::PeriodicExecutionContext::Com
p*, std::vector<RTC::PeriodicExecutionContext::Comp, std::allocator<RTC::PeriodicExecutionContext::Comp> > >, __gnu_cxx::__norm
al_iterator<RTC::PeriodicExecutionContext::Comp*, std::vector<RTC::PeriodicExecutionContext::Comp, std::allocator<RTC::PeriodicEx
ecutionContext::Comp> > >, RTC::PeriodicExecutionContext::invoke_worker) /usr/include/c++/5/bits/stl_algo.h:3767
04:53:18 #4 0x7ffb31448be8 in cnoid::ChoreonoidExecutionContext::tick() /home/jenkinshrg/src/choreonoid/src/OpenRT
lugin/ChoreonoidExecutionContext.cpp:35
04:53:18 #5 0x7ffb2fb7d94e in omni::omniOrbPOA::dispatch(omniCallDescriptor&, omniLocalIdentity*) (/usr/lib/libomni
4.so.1+0xe494e)
04:53:18 #6 0x7ffb2fb62938 in omniLocalIdentity::dispatch(omniCallDescriptor&) (/usr/lib/libomniORB4.so.1+0xc9938)
04:53:18 #7 0x7ffb2fb70a64 in omniObjRef::_invoke(omniCallDescriptor&, bool) (/usr/lib/libomniORB4.so.1+0xd7a64)
04:53:18 #8 0x7ffb30b638fc in OpenRTM::_objref_ExtTrigExecutionContextService::tick() ../../../../src/lib/rtm/idl/OpenRTM
.cc:509
04:53:18 #9 0x7ffb314b2ff8 in cnoid::BodyRTCItem::control() /home/jenkinshrg/src/choreonoid/src/OpenRTMPlugin/dep
ated/BodyRTCItem.cpp:366
04:53:18 #10 0x7ffb37825813 in cnoid::SimulatorItemImpl::concurrentControlLoop() /home/jenkinshrg/src/choreonoid/s
BodyPlugin/SimulatorItem.cpp:2027
04:53:18 #11 0x7ffb65a35c7f (/usr/lib/x86_64-linux-gnu/libstdc++.so.6+0xb8c7f)
04:53:18 #12 0x7ffb651876b9 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76b9)
04:53:18 #13 0x7ffb654a43dc in clone (/lib/x86_64-linux-gnu/libc.so.6+0x1073dc)
04:53:18
04:53:18 0x6060003d6d10 is located 16 bytes inside of 64-byte region [0x6060003d6d00,0x6060003d6d40)
04:53:18 freed by thread T14 (QThread) here:
04:53:18 #0 0x7ffb6a7efcaa in operator delete[](void*) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99caa)
04:53:18 #1 0x7ffb30968acf in RTC_Utils::StateMachine<RTC::LifeCycleState, RTC::PeriodicExecutionContext::DFPBase, R
Utils::StateHolder<RTC::LifeCycleState>, void (RTC::PeriodicExecutionContext::DFPBase::*)(RTC_Utils::StateHolder<RTC::LifeCycleStat
e> const&)>::~StateMachine() ../../../src/lib/rtm/StateMachine.h:305
04:53:18 #2 0x7ffb30968acf in RTC::PeriodicExecutionContext::DFPBase::~DFPBase() ../../../src/lib/rtm/PeriodicExecutionC
ext.h:724
04:53:18 #3 0x7ffb30968acf in RTC::PeriodicExecutionContext::DFP<_CORBA_ObjRef_Var<OpenRTM::_objref_DataFlowCom
onent, OpenRTM::DataFlowComponent_Helper> >::~DFP() ../../../src/lib/rtm/PeriodicExecutionContext.h:1047
04:53:18 #4 0x7ffb30968acf in RTC::PeriodicExecutionContext::Comp::~Comp() ../../../src/lib/rtm/PeriodicExecutionContex
1376
04:53:18 #5 0x7ffb30968acf in void std::_Destroy<RTC::PeriodicExecutionContext::Comp>(RTC::PeriodicExecutionContext::C
```

```
mp*) /usr/include/c++/5/bits/stl_construct.h:93
04:53:18 #6 0x7ffb30968acf in void std::_Destroy_aux<false>::__destroy<RTC::PeriodicExecutionContext::Comp*>(RTC::Peri
cExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*) /usr/include/c++/5/bits/stl_construct.h:103
04:53:18 #7 0x7ffb30968acf in void std::_Destroy<RTC::PeriodicExecutionContext::Comp*>(RTC::PeriodicExecutionContext:
mp*, RTC::PeriodicExecutionContext::Comp*) /usr/include/c++/5/bits/stl_construct.h:126
04:53:18 #8 0x7ffb30968acf in void std::_Destroy<RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContex
mp>(RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*, std::allocator<RTC::PeriodicExecutionContext::
Comp>&) /usr/include/c++/5/bits/stl_construct.h:151
04:53:18 #9 0x7ffb30968acf in std::vector<RTC::PeriodicExecutionContext::Comp, std::allocator<RTC::PeriodicExecutionCon
t::Comp> >::_M_insert_aux(__gnu_cxx::__normal_iterator<RTC::PeriodicExecutionContext::Comp*, std::vector<RTC::PeriodicExecutio
nContext::Comp, std::allocator<RTC::PeriodicExecutionContext::Comp> > >, RTC::PeriodicExecutionContext::Comp const&) /usr/incl
ude/c++/5/bits/vector.tcc:392
04:53:18
04:53:18 previously allocated by thread T14 (QThread) here:
04:53:18 #0 0x7ffb6a7ef6b2 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x996b2)
04:53:18 #1 0x7ffb30967842 in RTC_Utils::StateMachine<RTC::LifeCycleState, RTC::PeriodicExecutionContext::DFPBase, R
Utils::StateHolder<RTC::LifeCycleState>, void (RTC::PeriodicExecutionContext::DFPBase::*)(RTC_Utils::StateHolder<RTC::LifeCycleStat
e> const&)>::StateMachine(int) ../../../src/lib/rtm/StateMachine.h:291
04:53:18 #2 0x7ffb30967842 in RTC::PeriodicExecutionContext::DFPBase::DFPBase(int) ../../../src/lib/rtm/PeriodicExecutio
ontext.h:692
04:53:18 #3 0x7ffb30967842 in RTC::PeriodicExecutionContext::DFP<_CORBA_ObjRef_Var<OpenRTM::_objref_DataFlowCom
onent, OpenRTM::DataFlowComponent_Helper> >::DFP(_CORBA_ObjRef_Var<OpenRTM::_objref_DataFlowComponent, OpenRTM::D
ataFlowComponent_Helper>, int) ../../../src/lib/rtm/PeriodicExecutionContext.h:1071
04:53:18 #4 0x7ffb30967842 in RTC::PeriodicExecutionContext::Comp::Comp(RTC::PeriodicExecutionContext::Comp const&
/../../src/lib/rtm/PeriodicExecutionContext.h:1379
04:53:18 #5 0x7ffb30967842 in void std::_Construct<RTC::PeriodicExecutionContext::Comp, RTC::PeriodicExecutionConte
omp>(RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp const&) /usr/include/c++/5/bits/stl_construct.
h:83
04:53:18 #6 0x7ffb30967842 in RTC::PeriodicExecutionContext::Comp* std::__uninitialized_copy<false>::__uninit_copy<RT
PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*>(RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicEx
ecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*) /usr/include/c++/5/bits/stl_uninitialized.h:75
04:53:18 #7 0x7ffb30967842 in RTC::PeriodicExecutionContext::Comp* std::uninitialized_copy<RTC::PeriodicExecutionCon
t::Comp*, RTC::PeriodicExecutionContext::Comp*>(RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*, R
TC::PeriodicExecutionContext::Comp*) /usr/include/c++/5/bits/stl_uninitialized.h:126
04:53:18 #8 0x7ffb30967842 in RTC::PeriodicExecutionContext::Comp* std::__uninitialized_copy_a<RTC::PeriodicExecution
ntext::Comp*, RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp>(RTC::PeriodicExecutionContext::Comp
*, RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*, std::allocator<RTC::PeriodicExecutionContext::Co
mp>&) /usr/include/c++/5/bits/stl_uninitialized.h:281
04:53:18 #9 0x7ffb30967842 in RTC::PeriodicExecutionContext::Comp* std::__uninitialized_move_if_noexcept_a<RTC::Peri
cExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*, std::allocator<RTC::PeriodicExecutionContext::Comp> >(RTC::Per
iodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*, std::allocator<RTC::P
eriodicExecutionContext::Comp>&) /usr/include/c++/5/bits/stl_uninitialized.h:304
04:53:18 #10 0x7ffb30967842 in std::vector<RTC::PeriodicExecutionContext::Comp, std::allocator<RTC::PeriodicExecutionC
text::Comp> >::_M_insert_aux(__gnu_cxx::__normal_iterator<RTC::PeriodicExecutionContext::Comp*, std::vector<RTC::PeriodicExecu
tionContext::Comp, std::allocator<RTC::PeriodicExecutionContext::Comp> > >, RTC::PeriodicExecutionContext::Comp const&) /usr/i
nclude/c++/5/bits/vector.tcc:370
04:53:18
04:53:18 Thread T12 created by T0 here:
04:53:18 #0 0x7ffb6a78c253 in pthread_create (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x36253)
04:53:18 #1 0x7ffb65a35dc2 in std::thread::_M_start_thread(std::shared_ptr<std::thread::_Impl_base>, void (*)()) (/usr/li
_64-linux-gnu/libstdc++.so.6+0xb8dc2)
04:53:18
04:53:18 Thread T14 (QThread) created by T0 here:
04:53:18 #0 0x7ffb6a78c253 in pthread_create (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x36253)
04:53:18 #1 0x7ffb65d84f89 in QThread::start(QThread::Priority) (/usr/local/Trolltech/Qt-4.8.6/lib/libQtCore.so.4+0x85f8
04:53:18
04:53:18 SUMMARY: AddressSanitizer: heap-use-after-free /home/jenkinshrg/openrtp/include/openrtm-1.1/rtm/StateMachine.h:
698 RTC_Utils::StateMachine<RTC::LifeCycleState, RTC::PeriodicExecutionContext::DFPBase, RTC_Utils::StateHolder<RTC::LifeCycle
State>, void (RTC::PeriodicExecutionContext::DFPBase::*)(RTC_Utils::StateHolder<RTC::LifeCycleState> const&)>::worker()
04:53:18 Shadow bytes around the buggy address:
04:53:18 0x0c0c80072d50: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
04:53:18 0x0c0c80072d60: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
04:53:18 0x0c0c80072d70: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
04:53:18 0x0c0c80072d80: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
04:53:18 0x0c0c80072d90: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
04:53:18 =>0x0c0c80072da0: fd fd[fd]fd fd fd fd fd fa fa fa fa fd fd fd fd
04:53:18 0x0c0c80072db0: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
```

```
04:53:18        0x0c0c80072dc0: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
04:53:18        0x0c0c80072dd0: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
04:53:18        0x0c0c80072de0: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
04:53:18        0x0c0c80072df0: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
04:53:18  Shadow byte legend (one shadow byte represents 8 application bytes):
04:53:18        Addressable:                    00
04:53:18        Partially addressable: 01 02 03 04 05 06 07
04:53:18        Heap left redzone:               fa
04:53:18        Heap right redzone:              fb
04:53:18        Freed heap region:               fd
04:53:18        Stack left redzone:              f1
04:53:18        Stack mid redzone:               f2
04:53:18        Stack right redzone:             f3
04:53:18        Stack partial redzone:           f4
04:53:18        Stack after return:              f5
04:53:18        Stack use after scope:           f8
04:53:18        Global redzone:                  f9
04:53:18        Global init order:               f6
04:53:18        Poisoned by user:                f7
04:53:18        Container overflow:              fc
04:53:18        Array cookie:                    ac
04:53:18        Intra object redzone:            bb
04:53:18        ASan internal:                   fe
04:53:18  ==20889==ABORTING
```

## 履歴

### #1 - 2017/10/18 10:17 - n-ando

金広様

見た感じ、Choreonoidから EC の tick を読んだ後に、
RTCのコールバックが呼ばれる前に、別スレッドで
コンポーネント？EC？をDeleteしているみたいですね。
cnoid::BodyRTCItem を削除している部分周りで
そのようなコードがありますでしょうか？
こちらでも、あとで見てみます。

安藤

### #2 - 2017/10/18 10:46 - kanehiro

タイミングとしては、シミュレーションを走らせながら、色んなRTCを作ったり、ポート接続したりしているところで、BodyRTCItemの削除はしていないと思います。