

OpenRTM-aist (C++) - バグ #4410

Address Sanitizerがheap use after freeを検出

2018/01/09 09:31 - kanehiro

ステータス:	新規	開始日:	2018/01/09
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

再現性がないのですが、Address Sanitizerがheap use after freeを検出したので報告しておきます。
releng_1_1を使用しています。

```
==9380==ERROR: AddressSanitizer: heap-use-after-free on address 0x6060003f19b0 at pc 0x7f5a71ab3779 bp 0x7f5a996e0 sp 0x7f5a996636d0
READ of size 8 at 0x6060003f19b0 thread T12
#0 0x7f5a71ab3778 in RTC_Utils::StateMachine<RTC::LifeCycleState, RTC::PeriodicExecutionContext::DFPBase, RTC_Utils::StateHolder<RTC::LifeCycleState>, void (RTC::PeriodicExecutionContext::DFPBase::*)(RTC_Utils::StateHolder<RTC::LifeCycleState> const&)>::worker() /home/jenkinshrng/openrtm/include/openrtm-1.1/rtm/StateMachine.h:698
#1 0x7f5a71ab3778 in RTC::PeriodicExecutionContext::DFPBase::worker() /home/jenkinshrng/openrtm/include/openrtm-1.1/rtm/PeriodicExecutionContext.h:978
#2 0x7f5a71ab3778 in RTC::PeriodicExecutionContext::invoke_worker::operator()(RTC::PeriodicExecutionContext::Comp&) /home/jenkinshrng/openrtm/include/openrtm-1.1/rtm/PeriodicExecutionContext.h:1467
#3 0x7f5a71ab3778 in RTC::PeriodicExecutionContext::invoke_worker std::for_each<__gnu_cxx::__normal_iterator<RTC::PeriodicExecutionContext::Comp*, std::vector<RTC::PeriodicExecutionContext::Comp, std::allocator<RTC::PeriodicExecutionContext::Comp>>, RTC::PeriodicExecutionContext::invoke_worker>(__gnu_cxx::__normal_iterator<RTC::PeriodicExecutionContext::Comp*, std::vector<RTC::PeriodicExecutionContext::Comp, std::allocator<RTC::PeriodicExecutionContext::Comp>>>, __gnu_cxx::__normal_iterator<RTC::PeriodicExecutionContext::Comp*, std::vector<RTC::PeriodicExecutionContext::Comp, std::allocator<RTC::PeriodicExecutionContext::Comp>>>, RTC::PeriodicExecutionContext::invoke_worker) /usr/include/c++/5/bits/stl_algo.h:3767
#4 0x7f5a71ab3778 in cnoid::ChoreonoidExecutionContext::tick() /home/jenkinshrng/src/choreonoid/src/OpenRTMPlugin/ChoreonoidExecutionContext.cpp:35
#5 0x7f5a727ac94e in omni::omniOrbPOA::dispatch(omniCallDescriptor&, omniLocalIdentity*) (/usr/lib/libomniORB4.so.1+0xe494e)
#6 0x7f5a72791938 in omniLocalIdentity::dispatch(omniCallDescriptor&) (/usr/lib/libomniORB4.so.1+0xc9938)
#7 0x7f5a7279fa64 in omniObjRef::_invoke(omniCallDescriptor&, bool) (/usr/lib/libomniORB4.so.1+0xd7a64)
#8 0x7f5a70b4c8fc in OpenRTM::_objref_ExtTrigExecutionContextService::tick() ../../src/lib/rtm/idl/OpenRTMSK.cc:509
#9 0x7f5a71b1e2a8 in cnoid::BodyRTCItem::control() /home/jenkinshrng/src/choreonoid/src/OpenRTMPlugin/deprecated/BodyRTCItem.cpp:378
#10 0x7f5a6f25fa43 in cnoid::SimulatorItemImpl::concurrentControlLoop() /home/jenkinshrng/src/choreonoid/src/BodyPlugin/SimulatorItem.cpp:2081
#11 0x7f5aa62e1c7f (/usr/lib/x86_64-linux-gnu/libstdc++.so.6+0xb8c7f)
#12 0x7f5aa5a336b9 in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76b9)
#13 0x7f5aa5d503dc in clone (/lib/x86_64-linux-gnu/libc.so.6+0x1073dc)

0x6060003f19b0 is located 16 bytes inside of 64-byte region [0x6060003f19a0,0x6060003f19e0)
freed by thread T14 (QThread) here:
#0 0x7f5aab09bcaa in operator delete[](void*) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99caa)
#1 0x7f5a70951acf in RTC_Utils::StateMachine<RTC::LifeCycleState, RTC::PeriodicExecutionContext::DFPBase, RTC_Utils::StateHolder<RTC::LifeCycleState>, void (RTC::PeriodicExecutionContext::DFPBase::*)(RTC_Utils::StateHolder<RTC::LifeCycleState> const&)>::StateMachine() ../../src/lib/rtm/StateMachine.h:305
#2 0x7f5a70951acf in RTC::PeriodicExecutionContext::DFPBase::~DFPBase() ../../src/lib/rtm/PeriodicExecutionContext.h:72
#3 0x7f5a70951acf in RTC::PeriodicExecutionContext::DFP<_CORBA_ObjRef_Var<OpenRTM::_objref_DataFlowComponent, OpenRTM::DataFlowComponent_Helper>>::DFP() ../../src/lib/rtm/PeriodicExecutionContext.h:1047
#4 0x7f5a70951acf in RTC::PeriodicExecutionContext::Comp::Comp() ../../src/lib/rtm/PeriodicExecutionContext.h:1376
#5 0x7f5a70951acf in void std::_Destroy<RTC::PeriodicExecutionContext::Comp>(RTC::PeriodicExecutionContext::Comp*) /usr/include/c++/5/bits/stl_construct.h:93
#6 0x7f5a70951acf in void std::_Destroy_aux<false>::_destroy<RTC::PeriodicExecutionContext::Comp*>(RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*) /usr/include/c++/5/bits/stl_construct.h:103
#7 0x7f5a70951acf in void std::_Destroy<RTC::PeriodicExecutionContext::Comp*>(RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*) /usr/include/c++/5/bits/stl_construct.h:126
#8 0x7f5a70951acf in void std::_Destroy<RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp>(R
```

```

PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*, std::allocator<RTC::PeriodicExecutionContext::Comp*>) /
usr/include/c++/5/bits/stl_construct.h:151
#9 0x7f5a70951acf in std::vector<RTC::PeriodicExecutionContext::Comp, std::allocator<RTC::PeriodicExecutionContext::Comp>
>::_M_insert_aux(__gnu_cxx::__normal_iterator<RTC::PeriodicExecutionContext::Comp*, std::vector<RTC::PeriodicExecutionContext::
Comp, std::allocator<RTC::PeriodicExecutionContext::Comp> >, RTC::PeriodicExecutionContext::Comp const&)/usr/include/c++/5
/bits/vector.tcc:392

previously allocated by thread T14 (QThread) here:
#0 0x7f5aab09b6b2 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x996b2)
#1 0x7f5a70950842 in RTC_Utils::StateMachine<RTC::LifeCycleState, RTC::PeriodicExecutionContext::DFPBase, RTC_Utils::
eHolder<RTC::LifeCycleState>, void (RTC::PeriodicExecutionContext::DFPBase::*)(RTC_Utils::StateHolder<RTC::LifeCycleState> const
&)>::StateMachine(int) ../../src/lib/rtm/StateMachine.h:291
#2 0x7f5a70950842 in RTC::PeriodicExecutionContext::DFPBase::DFPBase(int) ../../src/lib/rtm/PeriodicExecutionContext.h
92
#3 0x7f5a70950842 in RTC::PeriodicExecutionContext::DFP<_CORBA_ObjRef_Var<OpenRTM::_objref_DataFlowComponent,
penRTM::DataFlowComponent_Helper> >::DFP(_CORBA_ObjRef_Var<OpenRTM::_objref_DataFlowComponent, OpenRTM::DataFlow
Component_Helper>, int) ../../src/lib/rtm/PeriodicExecutionContext.h:1071
#4 0x7f5a70950842 in RTC::PeriodicExecutionContext::Comp::Comp(RTC::PeriodicExecutionContext::Comp const&) ../../s
ib/rtm/PeriodicExecutionContext.h:1379
#5 0x7f5a70950842 in void std::_Construct<RTC::PeriodicExecutionContext::Comp, RTC::PeriodicExecutionContext::Comp>
C::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp const&)/usr/include/c++/5/bits/stl_construct.h:83
#6 0x7f5a70950842 in RTC::PeriodicExecutionContext::Comp* std::_uninitialized_copy<false>::__uninit_copy<RTC::Periodic
ecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*>(RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecu
tionContext::Comp*, RTC::PeriodicExecutionContext::Comp*) /usr/include/c++/5/bits/stl_uninitialized.h:75
#7 0x7f5a70950842 in RTC::PeriodicExecutionContext::Comp* std::_uninitialized_copy<RTC::PeriodicExecutionContext::Comp
RTC::PeriodicExecutionContext::Comp*>(RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*, RTC::Perio
dicExecutionContext::Comp*) /usr/include/c++/5/bits/stl_uninitialized.h:126
#8 0x7f5a70950842 in RTC::PeriodicExecutionContext::Comp* std::_uninitialized_copy_a<RTC::PeriodicExecutionContext::C
mp*, RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp>(RTC::PeriodicExecutionContext::Comp*, RTC::P
eriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*, std::allocator<RTC::PeriodicExecutionContext::Comp>&)/u
sr/include/c++/5/bits/stl_uninitialized.h:281
#9 0x7f5a70950842 in RTC::PeriodicExecutionContext::Comp* std::_uninitialized_move_if_noexcept_a<RTC::PeriodicExecu
nContext::Comp*, RTC::PeriodicExecutionContext::Comp*, std::allocator<RTC::PeriodicExecutionContext::Comp> >(RTC::PeriodicExc
utionContext::Comp*, RTC::PeriodicExecutionContext::Comp*, RTC::PeriodicExecutionContext::Comp*, std::allocator<RTC::PeriodicEx
ecutionContext::Comp>&)/usr/include/c++/5/bits/stl_uninitialized.h:304
#10 0x7f5a70950842 in std::vector<RTC::PeriodicExecutionContext::Comp, std::allocator<RTC::PeriodicExecutionContext::Comp>
>::_M_insert_aux(__gnu_cxx::__normal_iterator<RTC::PeriodicExecutionContext::Comp*, std::vector<RTC::PeriodicExecutionContext::Comp,
std::allocator<RTC::PeriodicExecutionContext::Comp> >, RTC::PeriodicExecutionContext::Comp const&)/usr/include/c++
/5/bits/vector.tcc:370

Thread T12 created by T0 here:
#0 0x7f5aab038253 in pthread_create (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x36253)
#1 0x7f5aa62e1dc2 in std::thread::_M_start_thread(std::shared_ptr<std::thread::_Impl_base>, void (*)()) (/usr/lib/x86_64-
-gnu/libstdc++.so.6+0xb8dc2)

Thread T14 (QThread) created by T0 here:
#0 0x7f5aab038253 in pthread_create (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x36253)
#1 0x7f5aa6630f89 in QThread::start(QThread::Priority) (/usr/local/Trolltech/Qt-4.8.6/lib/libQtCore.so.4+0x85f89)

SUMMARY: AddressSanitizer: heap-use-after-free /home/jenkinshrng/openrtm/include/openrtm-1.1/rtm/StateMachine.h:698 RTC_
Utils::StateMachine<RTC::LifeCycleState, RTC::PeriodicExecutionContext::DFPBase, RTC_Utils::StateHolder<RTC::LifeCycleState>, voi
d (RTC::PeriodicExecutionContext::DFPBase::*)(RTC_Utils::StateHolder<RTC::LifeCycleState> const&)>::worker()
Shadow bytes around the buggy address:
0x0c0c800762e0: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
0x0c0c800762f0: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
0x0c0c80076300: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
0x0c0c80076310: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
0x0c0c80076320: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0c0c80076330: fa fa fa fa fd fd[fd]fd fd fd fd fd fd fa fa fa fa
0x0c0c80076340: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
0x0c0c80076350: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
0x0c0c80076360: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
0x0c0c80076370: fd fd fd fd fd fd fd fd fa fa fa fd fd fd fd fd
0x0c0c80076380: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
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	
Heap	right	redzone:	fb	
Freed	heap	region:	fd	
Stack	left	redzone:	f1	
Stack	mid	redzone:	f2	
Stack	right	redzone:	f3	
Stack	partial	redzone:	f4	
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	
==9380==ABORTING				

履歴

#1 - 2018/01/10 15:24 - kanehiro

[#4270](#) で報告しているのと同じ原因のようですね。