

DCMTK - Bug #1137

Valgrind reports thread errors in multithreaded programs using oficonv

2024-09-18 13:13 - Marco Eichelberg

Status:	Closed	Start date:	2024-09-18
Priority:	Normal	Due date:	
Assignee:	Marco Eichelberg	% Done:	100%
Category:	Library and Apps	Estimated time:	2:00 hours
Target version:	3.7.1+	Compiler:	
Module:	oficonv		
Operating System:			

Description

The thread errors reported by valgrind can be reproduced with the following steps:

```
g++ -DNTHREADS=16 -o input_threads -g -O2 input_threads.cc -ldcmdata -lstd
export ICONV_MAX_REUSE=0
valgrind --tool=drd ./input_threads test_case.dcm
```

The output depends on the options with which DCMTK was compiled, but here is one possible output:

```
==1868338== drd, a thread error detector
==1868338== Copyright (C) 2006-2020, and GNU GPL'd, by Bart Van Assche.
==1868338== Using Valgrind-3.20.0 and LibVEX; rerun with -h for copyright info
==1868338== Command: ./input_threads /tmp/test_case.dcm
==1868338==
W==1868338== Thread 4:
==1868338== Conflicting store by thread 4 at 0x0551d880 size 8
==1868338==    at 0x4FE85A4: _iconv_open (oficonv_iconv.c:117)
==1868338==    by 0x4A9F1C6: UnknownInlinedFun (ofchrenc.cc:337)
==1868338==    by 0x4A9F1C6:
OFCharacterEncoding::selectEncoding(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&) (ofchrenc.cc:785)
==1868338==    by 0x49DD9AF:
DcmSpecificCharacterSet::selectCharacterSet(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&) (dcspchrs.cc:178)
==1868338==    by 0x49B6BBA:
DcmItem::convertCharacterSet(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&, unsigned long, bool) (dcitem.cc:4403)
==1868338==    by 0x49B405A:
DcmItem::convertCharacterSet(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&, unsigned long, bool) (dcitem.cc:4442)
==1868338==    by 0x1094DD: run(void*) (input_threads.cxx:26)
==1868338==    by 0x4850208: ??? (in
/usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==1868338==    by 0x4DE4731: start_thread (pthread_create.c:447)
==1868338==    by 0x4E5F0FF: clone (clone.S:100)
==1868338== Address 0x551d880 is at offset 80 from 0x551d830.
Allocation context:
==1868338==    at 0x4849A28: malloc (in
/usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==1868338==    by 0x4FE2375: UnknownInlinedFun (citrus_iconv.c:159)
==1868338==    by 0x4FE2375: UnknownInlinedFun (citrus_iconv.c:265)
==1868338==    by 0x4FE2375: _citrus_iconv_open (citrus_iconv.c:349)
==1868338==    by 0x4FE85DF: _iconv_open (oficonv_iconv.c:107)
==1868338==    by 0x4A9F1C6: UnknownInlinedFun (ofchrenc.cc:337)
==1868338==    by 0x4A9F1C6:
```

```

OFCharacterEncoding::selectEncoding(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&) (ofchrenc.cc:785)
==1868338== by 0x49DD9AF:
DcmSpecificCharacterSet::selectCharacterSet(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&) (dcspchrs.cc:178)
==1868338== by 0x49B6BBA:
DcmItem::convertCharacterSet(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&, unsigned long, bool) (dcitem.cc:4403)
==1868338== by 0x49B405A:
DcmItem::convertCharacterSet(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&, unsigned long, bool) (dcitem.cc:4442)
==1868338== by 0x1094DD: run(void*) (input_threads.cxx:26)
==1868338== by 0x4850208: ??? (in
/usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==1868338== by 0x4DE4731: start_thread (pthread_create.c:447)
==1868338== by 0x4E5F0FF: clone (clone.S:100)
==1868338== Other segment start (thread 2)
==1868338== at 0x485AC4F: pthread_mutex_unlock@* (in
/usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==1868338== by 0x492C5EF: UnknownInlinedFun (ofglobal.h:99)
==1868338== by 0x492C5EF:
DcmByteString::makeMachineByteString(unsigned int) (dcbystr.cc:596)
==1868338== by 0x492C4E8: DcmByteString::getString(char*&) (dcbystr.cc:427)
==1868338== by 0x4928720: DcmByteString::getString(char*&, unsigned
int&) (dcbystr.cc:436)
==1868338== by 0x492EA04:
DcmCharString::convertCharacterSet(DcmSpecificCharacterSet&)
(dcchrstr.cc:165)
==1868338== by 0x49B387A:
DcmItem::convertCharacterSet(DcmSpecificCharacterSet&)
(dcitem.cc:4455)
==1868338== by 0x49B6C4E:
DcmItem::convertCharacterSet(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&, unsigned long, bool) (dcitem.cc:4417)
==1868338== by 0x49B405A:
DcmItem::convertCharacterSet(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&, unsigned long, bool) (dcitem.cc:4442)
==1868338== by 0x1094DD: run(void*) (input_threads.cxx:26)
==1868338== by 0x4850208: ??? (in
/usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==1868338== by 0x4DE4731: start_thread (pthread_create.c:447)
==1868338== by 0x4E5F0FF: clone (clone.S:100)
==1868338== Other segment end (thread 2)
==1868338== at 0x486B1FC: pthread_rwlock_rdlock@* (in
/usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==1868338== by 0x4D91805: __dcigettext (dcigettext.c:567)
==1868338== by 0x4A9E014: UnknownInlinedFun (ofchrenc.cc:606)
==1868338== by 0x4A9E014:
OFCharacterEncoding::Implementation::convert(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >&, char const*, unsigned long) (ofchrenc.cc:566)
==1868338== by 0x4A9E1B0: OFCharacterEncoding::convertString(charconst*, unsigned long, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >&, bool)
(ofchrenc.cc:825)
==1868338== by 0x49E105E:
DcmSpecificCharacterSet::convertString(char const*, unsigned long, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >&, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&)
(dcspchrs.cc:558)
==1868338== by 0x492EAA3:
DcmCharString::convertCharacterSet(DcmSpecificCharacterSet&)
(dcchrstr.cc:171)
==1868338== by 0x49B387A:
DcmItem::convertCharacterSet(DcmSpecificCharacterSet&)

```

```
(dcitem.cc:4455)
==1868338==      by 0x49B6C4E:
DcmItem::convertCharacterSet(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&, unsigned long, bool) (dcitem.cc:4417)
==1868338==      by 0x49B405A:
DcmItem::convertCharacterSet(std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&, unsigned long, bool) (dcitem.cc:4442)
==1868338==      by 0x1094DD: run(void*) (input_threads.cxx:26)
==1868338==      by 0x4850208: ??? (in
/usr/libexec/valgrind/vgpreload_drd-amd64-linux.so)
==1868338==      by 0x4DE4731: start_thread (pthread_create.c:447)
==1868338==
```

It seems that `_citrus_iconv_open()` contains a race issue that will need further examination.

Thanks to Mathieu Malaterre <mathieu.malaterre@gmail.com> for the bug report and sample code, provided on 2024-09-02.

History

#1 - 2024-12-29 15:17 - Marco Eichelberg

- Status changed from New to Closed
- Assignee set to Marco Eichelberg
- % Done changed from 0 to 100
- Estimated time set to 2:00 h

Closed by commit #b88017dfc.

Files

input_threads.cc	1.25 KB	2024-09-18	Marco Eichelberg
test_case.dcm	257 KB	2024-09-18	Marco Eichelberg