DCMTK - Bug #646

storescu/scp crash in debug mode when using association negotiation profiles

2015-07-02 17:29 - Jörg Riesmeier

Status:	Closed	**Start date:**	2015-07-02
Priority:	High	**Due date:**	
Assignee:	Michael Onken	**% Done:**	100%
Category:	Library	**Estimated time:**	0:00 hour
Target version:	3.6.1+		
Module:	dcmnet	**Compiler:**	
Operating System:	Linux		

Description

The tools crash when compiled with debug mode enabled and when using the -xf option:

```
Program received signal SIGSEGV, Segmentation fault.
0x000000000050fbff in OFListBase::base_insert (this=0x7dcba0, pos=0x2e352e3830303031, newElem=0x7d
cc80) at oflist.cc:57
57              newElem->prev = pos->prev;
(gdb) where
#0  0x000000000050fbff in OFListBase::base_insert (this=0x7dcba0, pos=0x2e352e3830303031, newElem=
0x7dcc80) at oflist.cc:57
#1  0x0000000000440526 in OFList<DcmPresentationContextItem>::insert (this=0x7dcba0, position=...,
 x=...) at ../../ofstd/include/dcmtk/ofstd/oflist.h:294
#2  0x0000000000440157 in OFList<DcmPresentationContextItem>::push_back (this=0x7dcba0, x=...) at
../../ofstd/include/dcmtk/ofstd/oflist.h:393
#3  0x000000000043f7a6 in DcmPresentationContextMap::add (this=0x7fffffffd728, key=0x7d6ad0 "STORA
GECOMPRESSEDANDUNCOMPRESSED",
    abstractSyntaxUID=0x7dcae0 "ComputedRadiographyImageStorage", transferSyntaxKey=0x7dcb20 "JPEG
BASELINE") at dccfpcmp.cc:147
#4  0x000000000043926a in DcmAssociationConfiguration::addPresentationContext (this=0x7fffffffd710
, key=0x7d6ad0 "STORAGECOMPRESSEDANDUNCOMPRESSED",
    abstractSyntaxUID=0x7dcae0 "ComputedRadiographyImageStorage", transferSyntaxKey=0x7dcb20 "JPEG
BASELINE") at dcasccfg.cc:97
#5  0x000000000043c208 in DcmAssociationConfigurationFile::parsePresentationContexts (cfg=..., con
fig=...) at dcasccff.cc:193
#6  0x000000000043b98e in DcmAssociationConfigurationFile::initialize (cfg=..., filename=0x7ccc60
"dcmnet/etc/storescu.cfg") at dcasccff.cc:72
#7  0x000000000040a1b1 in main (argc=7, argv=0x7fffffffddc8) at storescu.cc:470
```

Tested on Linux machine with gcc 4.8.4 and "./configure --enable-debug".

This issue is already present with DCMTK 3.6.0! (did not check any older versions)

History

#1 - 2015-07-02 17:36 - Jörg Riesmeier

- Description updated

#2 - 2015-07-10 12:00 - Jörg Riesmeier

Problem also occurs with older DCMTK versions (e.g. 3.5.3); seems to be an issue with the "memory protection" feature in Ubuntu/Mint Linux. However, the reason for the segmentation fault is probably a faulty implementation in the DCMTK (corrupted stack or heap).

Here are some details on the test system:

```
> lsb_release -a
LSB Version:    core-2.0-amd64:core-2.0-noarch:core-3.0-amd64:core-3.0-noarch:core-3.1-amd64:core-3.1-noarch:c
ore-3.2-amd64:core-3.2-noarch:core-4.0-amd64:core-4.0-noarch:core-4.1-amd64:core-4.1-noarch:cxx-3.0-amd64:cxx-
3.0-noarch:cxx-3.1-amd64:cxx-3.1-noarch:cxx-3.2-amd64:cxx-3.2-noarch:cxx-4.0-amd64:cxx-4.0-noarch:cxx-4.1-amd6
4:cxx-4.1-noarch:desktop-3.1-amd64:desktop-3.1-noarch:desktop-3.2-amd64:desktop-3.2-noarch:desktop-4.0-amd64:d
esktop-4.0-noarch:desktop-4.1-amd64:desktop-4.1-noarch:graphics-2.0-amd64:graphics-2.0-noarch:graphics-3.0-amd
64:graphics-3.0-noarch:graphics-3.1-amd64:graphics-3.1-noarch:graphics-3.2-amd64:graphics-3.2-noarch:graphics-
```

```
4.0-amd64:graphics-4.0-noarch:graphics-4.1-amd64:graphics-4.1-noarch:languages-3.2-amd64:languages-3.2-noarch:
languages-4.0-amd64:languages-4.0-noarch:languages-4.1-amd64:languages-4.1-noarch:multimedia-3.2-amd64:multime
dia-3.2-noarch:multimedia-4.0-amd64:multimedia-4.0-noarch:multimedia-4.1-amd64:multimedia-4.1-noarch:printing-
3.2-amd64:printing-3.2-noarch:printing-4.0-amd64:printing-4.0-noarch:printing-4.1-amd64:printing-4.1-noarch:qt
4-3.1-amd64:qt4-3.1-noarch:security-4.0-amd64:security-4.0-noarch:security-4.1-amd64:security-4.1-noarch
Distributor ID: LinuxMint
Description:    Linux Mint 17.1 Rebecca
Release:        17.1
Codename:       rebecca
```

And on the compiler used:

```
> gcc -v
Using built-in specs.
COLLECT_GCC=gcc
COLLECT_LTO_WRAPPER=/usr/lib/gcc/x86_64-linux-gnu/4.8/lto-wrapper
Target: x86_64-linux-gnu
Configured with: ../src/configure -v --with-pkgversion='Ubuntu 4.8.4-2ubuntu1~14.04' --with-bugurl=file:///usr
/share/doc/gcc-4.8/README.Bugs --enable-languages=c,c++,java,go,d,fortran,objc,obj-c++ --prefix=/usr --program
-suffix=-4.8 --enable-shared --enable-linker-build-id --libexecdir=/usr/lib --without-included-gettext --enabl
e-threads=posix --with-gxx-include-dir=/usr/include/c++/4.8 --libdir=/usr/lib --enable-nls --with-sysroot=/ --
enable-clocale=gnu --enable-libstdcxx-debug --enable-libstdcxx-time=yes --enable-gnu-unique-object --disable-l
ibmudflap --enable-plugin --with-system-zlib --disable-browser-plugin --enable-java-awt=gtk --enable-gtk-cairo
 --with-java-home=/usr/lib/jvm/java-1.5.0-gcj-4.8-amd64/jre --enable-java-home --with-jvm-root-dir=/usr/lib/jv
m/java-1.5.0-gcj-4.8-amd64 --with-jvm-jar-dir=/usr/lib/jvm-exports/java-1.5.0-gcj-4.8-amd64 --with-arch-direct
ory=amd64 --with-ecj-jar=/usr/share/java/eclipse-ecj.jar --enable-objc-gc --enable-multiarch --disable-werror
--with-arch-32=i686 --with-abi=m64 --with-multilib-list=m32,m64,mx32 --with-tune=generic --enable-checking=rel
ease --build=x86_64-linux-gnu --host=x86_64-linux-gnu --target=x86_64-linux-gnu
Thread model: posix
gcc version 4.8.4 (Ubuntu 4.8.4-2ubuntu1~14.04)
```

#3 - 2015-07-10 12:39 - Jörg Riesmeier

Additional note: Compiling with -fno-stack-protector "solves" this issue, i.e. there is not segmentation fault anymore.

See also: https://wiki.ubuntu.com/Security/Features

#4 - 2015-07-13 14:31 - Marco Eichelberg

The bug can be reproduced on Caesar (Debian 8.1 x64, gcc 4.9.2) when compiling with the flags -g -fstack-protector-all.
A call to ./storescp -xf ../etc/storescp.cfg default 10004 -v will immediately cause a segmentation fault.

The problem seems to be due to heap corruption occuring in DcmPresentationContextMap::add() (dcmnet/libsrc/dccfpcmp.cc).
On line 131 a new instance of class DcmPresentationContextList is created on the heap, and "value" points to it.
Line 147 reads (*value)->push_back(DcmPresentationContextItem(uid, OFString(transferSyntaxKey)));
In the debugger, you can see that at the beginning of the line, **value still is an intact and empty list,
but after completion of the constructors, and prior to the entry into push_back(), the list is damaged (overwritten).

#5 - 2015-09-04 11:52 - Marco Eichelberg

- Target version changed from 3.6.1 to 3.6.1+

#6 - 2016-11-25 08:13 - Michael Onken

- Assignee set to Michael Onken

#7 - 2017-01-27 17:38 - Jörg Riesmeier

- Operating System set to Linux

Also dcmrecv crashes in debug mode when started without --config-file, i.e. without an association negotiation profile, since internally the Verification SOP Class is added:

```
(gdb) r -v 9876
Starting program: ./dcmrecv -v 9876
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGSEGV, Segmentation fault.
0x0000000000522ce1 in OFListBase::base_insert (this=0x8fa320, pos=0x2e312e3830303031, newElem=0x8fa400) at ofl
ist.cc:57
57              newElem->prev = pos->prev;
(gdb) where
#0  0x0000000000522ce1 in OFListBase::base_insert (this=0x8fa320, pos=0x2e312e3830303031, newElem=0x8fa400) at
```

```
 oflist.cc:57
#1  0x000000000044b17a in OFList<DcmPresentationContextItem>::insert (this=0x8fa320, position=..., x=...) at .
./../ofstd/include/dcmtk/ofstd/oflist.h:294
#2  0x000000000044adc7 in OFList<DcmPresentationContextItem>::push_back (this=0x8fa320, x=...) at ../../ofstd/
include/dcmtk/ofstd/oflist.h:393
#3  0x000000000044a416 in DcmPresentationContextMap::add (this=0x7ff1c8, key=0x8fa2b0 "DEFAULT_PCKEY", abstrac
tSyntaxUID=0x8fa0e0 "1.2.840.10008.1.1", transferSyntaxKey=0x8fa140 "TSKEY_0") at dccfpcmp.cc:170
#4  0x0000000000443026 in DcmAssociationConfiguration::addPresentationContext (this=0x7ff1b0, key=0x8fa2b0 "DE
FAULT_PCKEY", abstractSyntaxUID=0x8fa0e0 "1.2.840.10008.1.1", transferSyntaxKey=0x8fa140 "TSKEY_0") at dcasccf
g.cc:97
#5  0x0000000000421919 in DcmSCPConfig::addPresentationContext (this=0x7ff1b0, abstractSyntax=..., xferSyntaxe
s=..., role=ASC_SC_ROLE_DEFAULT, profile=...) at scpcfg.cc:392
#6  0x000000000041e8ca in DcmSCP::addPresentationContext (this=0x7fffffffda50, abstractSyntax=..., xferSyntaxe
s=..., role=ASC_SC_ROLE_DEFAULT, profile=...) at scp.cc:1655
#7  0x00000000000408dae in DcmStorageSCP::DcmStorageSCP (this=0x7fffffffda50) at dstorscp.cc:52
#8  0x0000000000407a0e in main (argc=3, argv=0x7fffffffde48) at dcmrecv.cc:260
```

#8 - 2017-02-06 14:21 - Michael Onken

- Status changed from New to Closed

- % Done changed from 0 to 100

Closed by commit 77e93ca.