DCMTK - Bug #376

Possible buffer overflow in addOverrideKey()

2010-05-18 00:00 - Jörg Riesmeier

Status:	Closed	**Start date:**	
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:			
Module:	dcmnet + weitere	**Compiler:**	
Operating System:			

Description

http://forum.dcmtk.org/viewtopic.php?t=2523
At least the following tools are affected:

movescu
wltests
snd2dcm

'DcmPath' & Co. are likely culprits.

The former ones should be done, I haven't seen a sscanf() with a "%s" in DcmPath - Uli

=== Comment Uli ===

Find all instances, where sscanf() is used with s or something else (only %s happens though): git grep sscanf | grep -E '[^%"]*s'

```
dcmqrdb/libsrc/dcmqrcnf.cc: if (sscanf(rcline, "%s", mnemonic) != 1) dcmqrdb/libsrc/dcmqrcnf.cc: s
sscanf(valueptr, "%s", value); dcmqrdb/libsrc/dcmqrcnf.cc: sscanf(valueptr, "%s", value);
dcmqrdb/libsrc/dcmqrcnf.cc: sscanf(valueptr, "%s", value); dcmqrdb/libsrc/dcmqrcnf.cc: sscanf(rcli
ne, "%s %s", mnemonic, value); dcmqrdb/libsrc/dcmqrcnf.cc: sscanf(rcline, "%s %s", mnemonic, value
);
dcmqrdb/libsrc/dcmqrcnf.cc: sscanf(rcline, "%s %s", mnemonic, value); dcmqrdb/libsrc/dcmqrcnf.cc:
sscanf(helpvalue, "%d , %s", &studies, helpval); dcmqrdb/libsrc/dcmqrtis.cc: narg = sscanf(cmdbuf,
 "send %s %d", cmdarg, &iarg);
Found in dcmdata/libsrc/dcddirif.cc, dcmnet/apps/movescu.cc, dcmwlm/tests/wltests.cc und dcmwave/a
pps/snd2dcm.cc.
```

History

#1 - 2013-04-23 10:19 - Andrew Chiw

Possible buffer overflow in addOverrideKey()
Description

http://forum.dcmtk.org/viewtopic.php?t=2523
At least the following tools are affected:

```
movescu
    wltests
    snd2dcm
```

'DcmPath' & Co. are likely culprits.

The former should be settled, I haven't seen a sscanf() with a "%s" in DcmPath -- Uli

=== Comment Uli ===

Find all instances, where sscanf() is used with s or something else (only %s happens though): git grep sscanf | grep -E '[^%"]*s'
dcmqrdb/libsrc/dcmqrcnf.cc: if (sscanf(rcline, "%s", mnemonic) != 1) dcmqrdb/libsrc/dcmqrcnf.cc: sscanf(valueptr, "%s", value);
dcmqrdb/libsrc/dcmqrcnf.cc: sscanf(valueptr, "%s", value); dcmqrdb/libsrc/dcmqrcnf.cc: sscanf(valueptr, "%s", value); dcmqrdb/libsrc/dcmqrcnf.cc:
sscanf(rcline, "%s %s", mnemonic, value); dcmqrdb/libsrc/dcmqrcnf.cc: sscanf(rcline, "%s %s", mnemonic, value); dcmqrdb/libsrc/dcmqrcnf.cc:
sscanf(rcline, "%s %s", mnemonic, value); dcmqrdb/libsrc/dcmqrcnf.cc: sscanf(helpvalue, "%d , %s", &studies, helpval); dcmqrdb/libsrc/dcmqrtis.cc:
narg = sscanf(cmdbuf, "send %s %d", cmdarg, &iarg);

Found in dcmdata/libsrc/dcddirif.cc, dcmnet/apps/movescu.cc, dcmwlm/tests/wltests.cc und dcmwave/apps/snd2dcm.cc.

#2 - 2016-11-24 17:44 - Marco Eichelberg

- Status changed from New to Closed

All remaining instances of sscanf with %s parameter in the toolkit were checked, dcmqrdb is the only module using doing this, however, only on a string of known maximum size and not on an input line. Increased some buffer sizes to guarantee that no buffer overflows are possible.
Commit 22206bc thus closes this bug.