DCMTK - Bug #536

Crash during negotiation if Role Selection Item has a UID length of 0

2013-07-25 21:00 - Andreas Thiel

Status:	Closed	**Start date:**	2013-07-25
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library	**Estimated time:**	0:00 hour
Target version:	3.6.2		
Module:	dcmnet	**Compiler:**	
Operating System:			

Description

In cases were an application sends a Associate Request with some wrong content, the application crashes.
Mathieu Malaterre reported this effect with storescp.

Example of the crash:

```
D: PDU Type: Associate Request, PDU Length: 237 + 6 bytes PDU header
D:   01  00  00  00  00  ed  00  01  00  00  47  44  43  4d  5f  53
D:   54  4f  52  45  20  20  20  20  20  20  47  44  43  4d  44  41
D:   53  48  33  20  20  20  20  20  20  20  00  00  00  00  00  00
D:   00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
D:   00  00  00  00  00  00  00  00  00  00  10  00  00  15  31  2e
D:   32  2e  38  34  30  2e  31  30  30  30  38  2e  33  2e  31  2e
D:   31  2e  31  20  00  00  36  01  00  00  00  30  00  00  19  31
D:   2e  32  2e  38  34  30  2e  31  30  30  30  38  2e  35  2e  31
D:   2e  34  2e  31  2e  31  2e  34  40  00  00  11  31  2e  32  2e
D:   38  34  30  2e  31  30  30  30  38  2e  31  2e  32  50  00  00
D:   52  51  00  00  04  00  00  40  00  52  00  00  30  31  2e  32
D:   2e  38  32  36  2e  30  2e  31  2e  33  36  38  30  30  34  33
D:   2e  32  2e  31  31  34  33  2e  31  30  37  2e  31  30  34  2e
D:   31  30  33  2e  31  31  35  2e  32  2e  32  2e  33  54  00  00
D:   04  00  00  31  2e  32  2e  38  34  30  2e  31  30  30  30  38
D:   2e  35  2e
```

At the end there is the incomming item roleselectionitem

```
54  00  00  04  00  00  31  2e  32  2e  38  34  30  2e  31  30  30  30  38 2e
35  2e
```

With Length 4
And a UID length of 0

Logfile:

```
...
T: Subitem parse: Type 54, Length 0004, Content:  49 46
T: Parsing remaining 14 bytes of User Information
T: Next item type: 32
T: Parsing remaining 6 bytes of User Information
T: Next item type: 30
T: Parsing remaining 65534 bytes of User Information
T: Next item type: 00
T: Parsing remaining 65530 bytes of User Information
T: Parsing remaining 65526 bytes of User Information
T: Next item type: 00
T: Parsing remaining 65522 bytes of User Information
T: Next item type: 00
T: Parsing remaining 65518 bytes of User Information
T: Next item type: 00
T: Parsing remaining 65514 bytes of User Information
T: Next item type: 00
```

...

This wrong message should be recognized by dcmtk and either ignored or the connection have to be rejected.
Ideally the stack should recognize such pdu missmatch (wrong length of the item 54 coding, no uid length wrong scp/scu role) and stop trying to parse the rest of the pdu.

History

#1 - 2013-07-25 21:39 - Jörg Riesmeier

- Tracker changed from Feature to Bug

A crash is not a feature but a bug ;)

#2 - 2013-08-15 19:19 - Jörg Riesmeier

- Subject changed from Crash during negotiation if roleselction Item as a UID length of 0. to Crash during negotiation if Role Selection Item has a UID length of 0

#3 - 2017-04-16 14:35 - Marco Eichelberg

- File dcmtk_issue_536.bin added

- Status changed from New to Closed

- Assignee set to Marco Eichelberg

- % Done changed from 0 to 100

This bug has already been fixed by commit 1b6bb760 (December 2015), which fixed
several overflows/underflows in the ACSE code.

Attached is a file that can be sent to storescp using netcat and reproduces
the crash with storescp on DCMTK 3.6.0, but only leads to an error message
with newer versions:

Shell 1: storescp -ll trace 10000
Shell 2: netcat localhost 10000 <dcmtk_issue_536.bin

Closing this issue.

Files

s.log.gz	64.5 KB	2013-07-25	Andreas Thiel
storescp.cfg	8.34 KB	2013-07-25	Andreas Thiel
dcmtk_issue_536.bin	243 Bytes	2017-04-16	Marco Eichelberg