DCMTK - Feature #790

DCMTK 3.6.2 does not accept network connections with TLS 1.2 when compiled with OpenSSL < 1.1.0

2017-09-20 17:02 - Marco Eichelberg

Status:	Closed	**Start date:**	2017-09-20
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library	**Estimated time:**	0:00 hour
Target version:	3.6.3		
Module:	dcmtls	**Compiler:**	
Operating System:			

Description

DCMTK 3.6.2 does not accept network connections with TLS 1.2 when compiled with OpenSSL < 1.1.0
The reason is that for older versions of OpenSSL, the following methods are called, which explicitly only support TLS 1.0:

- TLSv1_server_method(), TLSv1_client_method(), TLSv1_method()

So neither TLS 1.1 nor TLS 1.2 can be negotiated in this case. For older OpenSSL versions, preferrably the following methods should be used:

- SSLv23_server_method(), SSLv23_client_method(), SSLv23_method()

In order to avoid the insecure SSLv2 and SSLv3 protocols, only TLS cipher suites should be enabled using setCipherSuites(). Additionally, SSL_CTX_set_min_proto_version() should be called to set the minimum protocol to TLS1_VERSION.

History

#1 - 2017-10-26 14:47 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

SSL_CTX_set_min_proto_version() is not available on older OpenSSL versions.
We use SSL_CTX_set_options() instead to disable SSLv2 and SSLv3.

The modified code has been successfully tested for compatibility with
DCMTK 3.5.4, 3.6.0 and 3.6.2 Release.

Closed by commit e099196.

Files

dcmtk-3.6.1_20170228-SSL.patch	1021 Bytes	2017-09-20	Marco Eichelberg