Network Device Interpretation # 201664

SSL/TLS Version Testing

Status: ☒ *Active* ☐ *Inactive*

Date: *7-Feb-2017*

Type of Document: ☐ *Technical Decision* ☒ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☐ *Network iTC*

Affected Document(s): *NDcPP v1.0, FWcPP v1.0, ND SD v1.0*

Affected Section(s): *FCS_TLSS_EXT.1.2 & FCS_TLSS_EXT.2.2 and related Tests in SD*

Superseded Interpretation(s): *None*

Issue:

The [CPP_ND_v1.0] contains the following tests for FCS_TLSS_EXT.1.2 and FCS_TLSS_EXT.2.2:

The evaluator shall send a Client Hello requesting a connection with version SSL 1.0 and verify that the server denies the connection. The evaluator shall repeat this test with SSL 2.0, SSL 3.0, TLS 1.0, and any selected TLS versions.

The SSL 1.0 protocol was never publicly released and the test cannot be executed using the SSL 1.0 protocol.

Resolution:

`The NIT proposes the following changes which shall be implemented if accepted by the Network iTC (sentence to be removed in case this recommendation is accepted).`

The NIT acknowledges that SSL 1.0 shall not be part of FCS_TLSS_EXT.1.2 and FCS_TLSS_EXT.2.2. FCS_TLSS_EXT.1.2 and FCS_TLSS_EXT.2.2 shall therefore be rewritten as follows:

*"*The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [selection: *TLS 1.1, TLS 1.2, none*]."

The Test activities for FCS_TLSS_EXT.1.2 and FCS_TLSS_EXT.2.2 in the ND SD shall be rewritten as follows:

*"*The evaluator shall send a Client Hello requesting a connection for all mandatory and selected protocol versions in the SFR (e.g. by enumeration of protocol versions in a test client) and verify that the server denies the connection for each attempt."

Rationale:

See Issue section.

Further Action:

None

Action by Network iTC:

None