Network Device Interpretation # 201921

FCS_TLSC_EXT.1.1 5e test clarification

Status: ☒ *Active* ☐ *Inactive*

Date: *16-Dec-2019*

End of proposed Transition Period (to be updated after TR2TD process): *16-Jan-2020*

Type of Change: ☐ Immediate application ☒ Minor change ☐ Major change

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

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

Affected Document(s): *NDSDv2.1*

Affected Section(s): *FCS_TLSC_EXT.1.1*

Superseded Interpretation(s): *None*

Issue:

The FCS_TLSC_EXT.1.1 5e test states:

e) Modify a byte in the Server Finished handshake message, and verify that the client sends an Encrypted Message followed by a FIN and ACK message. This is sufficient to deduce that the TOE responded with a Fatal Alert and no further data would be sent.

The observed behavior is that the client sends an Encrypted Alert message after the byte modification in the Server Finished handshake message, with the next message immediately following being a "RST and ACK" message sent from the server OR if the server is configured to not use the TCP RST flag to indicate an error, then either:

- *the server will send a "FIN and ACK" followed by the client (TOE) sending a "ACK" and "RST and ACK"; OR in some cases*
- *the client will send a "RST and ACK"*

In any of these cases, the TOE does not send Application Data after generating the Encrypted Alert message because the connection is effectively terminated with the RST message.

Proposal:

The test assurance activity should be modified as follows (underlined text represents the modification <got obviously lost in NIAP's tracking sheet>):

e) Modify a byte in the Server Finished handshake message, and verify that the client sends an Encrypted Message followed by either a FIN and ACK message or a RST and ACK message. This is sufficient to deduce that the TOE responded with a Fatal Alert and no further data would be sent.

Resolution:

To overcome the issue as described in the Issue section above, the definition of FCS_TLSC_EXT.1.1 Test 5e shall be modified as follows:

<old>" Modify a byte in the Server Finished handshake message, and verify that the client sends an Encrypted Message followed by a FIN and ACK message. This is sufficient to deduce that the TOE responded with a Fatal Alert and no further data would be sent."</old>

shall be replaced by

<new>" Modify a byte in the Server Finished handshake message, and verify that the handshake is not finished successfully and no application data flows."

Rationale:

The TLS tests in NDcPP have been analyzed by the TLSWG and an update proposal has been provided for NDcPP V2.2. One of the issues that have been found to be problematic multiple times was too strict definitions of expected responses by the TOE for negative testing. This comes at the risk of ruling out implementations which exhibit a comparable level of security but using a different implementation. Therefore, some test definitions have been generalized. The new test definition provided here reflects the updated proposal of the TLSWG for the particular test in NDcPP V2.1.

Further Action:

None

Action by Network iTC:

None