Network Device Interpretation # 202022

RFC Reference incorrect in TLSS Test

Status: ☒ *Active* ☐ *Inactive*

Date: *29-Oct-2020*

End of proposed Transition Period (to be updated after TR2TD process): *29-Nov-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): *NDSDv2.2*

Affected Section(s): *FCS_TLSS_EXT.1.4, Test 3*

Superseded Interpretation(s): *None*

Issue:

TLSS_EXT.1.4 test 3 NDcPP22e
The evaluator shall confirm that the TOE responds with a ServerHello that corresponds with either Figure 2 or Figure 3 of RFC 5077, which may or may not contain an empty SessionTicket extension or NewSessionTicket with ChangeCipherSpec and Finished messages as appropriate.
Consequently, test 3 part b.) states that "The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake (as shown in figure 3 or 4 of RFC 5077), or (2) terminates the connection in some way that prevents the flow of application data." Figure 3 of RFC 5077 represents a situation in which the server accepting a session ticket presented by the client in the Client Hello, but the server does not wish to renew the session ticket. Thus, test 3 part b.) should only refer to Figure 4 of RFC 5077, which shows a full handshake in the event that the server rejects the session ticket in the client's Client Hello:
The evaluator shall confirm that the TOE either (1) implicitly rejects the session ticket by performing a full handshake (as shown in figure 4 of RFC 5077), or (2) terminates the connection in some way that prevents the flow of application data.
From the CCTL's perspective, Test 3 part a.) of TLSS_EXT.1.4 in NDcPP22e should be changed to the following:
The evaluator shall confirm that the TOE either (1) responds with a ServerHello with an empty SessionTicket extension, NewSessionTicket, ChangeCipherSpec and Finished messages (as seen in figure 2 of RFC 5077) or (2) responds with a similar exchange, defined in Figure 2 of RFC 4346.
The test AA should be updated as such to align with what is permissible by RFC 5077.

Resolution:

The NIT acknowledges the two issues presented above.

The first issue refers to a possibly incorrect reference to Figure 3 with regards to FCS_TLSS_EXT.1.4 Test 3(b). The NIT disagrees with the issue as raised because figures 3 and 4 define scenarios when a SessionTicket may be rejected by the TOE's server while permitting flexibility in how the TOE Server may re-issue (or not) a NewSessionTicket.

The second issue above implicitly identifies a limitation in the message sequence for FCS_TLSS_EXT.1.4 test 3(a). The NIT acknowledges the issue and refers the reader to the resolution and rationale presented in NIT RFI 202024.

Rationale:

As described in the resolution above.

Further Action:

None

Action by Network iTC:

None