Network Device Interpretation # 202402a

Separation of test definitions for TLSv1.2 and v1.3 (renegotiation) (Client)

Status: ☒ *Active* ☐ *Inactive*

Date: *5-Aug-2024*

End of proposed Transition Period (to be updated after TR2TD process): *5-Sep-2024*

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): *NDSD v3.0e*

Affected Section(s): *FCS_TLSC_EXT.1.9, Test 4*

Superseded Interpretation(s): *None*

Issue:

Issue:

The test activity for TLS Clients, that reject renegotiation, are not accurate for TLS 1.2. Below is the associated SFR (FCS_TLSC_EXT.1.9) and Test (FCS_TLSC_EXT.1.9, Test 4):

The test activity for FCS_TLSC_EXT.1.9, Test 4 requires the TSF to terminate the TLS session after receiving a TLS 1.2 renegotiation request. For TLS 1.2, the TLS Client is required only to reject the request to renegotiate the TLS 1.2 session.

Specifically, a TOE with a TLS 1.2 Client does not take an action to terminate the TLS session when the TLS 1.2 Client does not support renegotiation and receives a Hello Request message. The TLS 1.2 Client is expected only to the ignore renegotiation request sent from the TLS server. No further action is required by the TLS 1.2 Client.

This behavior is different from TLS 1.3. When a TLS 1.3 Client receives a Hello Request, the TLS 1.3 Client is expected to issue a fatal alert (Unexpected Message) and terminate the TLS session. This is because in TLS 1.3 there is no support for renegotiation. Attempts to initiate TLS 1.2 renegotiation within a TLS 1.3 session are forbidden. For TOEs with a TLS 1.3 Client, the test activity for FCS_TLSC_EXT.1.9 Test 4 is accurate.

Proposed resolution:

FCS_TLSC_EXT.1.9, Test 4:

Test 4a [conditional, for TLS 1.3 only]: If "reject…renegotiation attempts" is selected, the evaluator shall initiate a TLS session between the so-configured TSF and a test server that is configured to perform a compliant handshake, followed by a hello reset request. The evaluator shall confirm that the TSF completes the initial handshake successfully but terminates the TLS session after receiving the hello request. Note: It is preferred that the TSF sends a fatal error alert message (e.g., unexpected message) in response to this, but it is acceptable that the TSF terminates the connection silently (i.e., without sending a fatal error alert).

Test 4b [conditional, for TLS 1.2 only]: If "reject…renegotiation attempts" is selected, the evaluator shall initiate a TLS session between the so-configured TSF and a test server that is configured to perform a compliant handshake, followed by a hello reset request. The evaluator shall confirm that the TSF completes the initial handshake successfully but does not initiate renegotiation after receiving the hello request.

Resolution:

The NIT acknowledges the issue. The following change shall be applied to the Supporting Document, Test Section for FCS_TLSC_EXT.1.9, Test 4:

{old}

Test 4 [conditional]: If "reject…renegotiation attempts" is selected, then for each selected TLS version, the evaluator shall initiate a TLS session between the so-configured TSF and a test server that is configured to perform a compliant handshake, followed by a hello reset request. The evaluator shall confirm that the TSF completes the initial handshake successfully but terminates the TLS session after receiving the hello reset request. Note: It is preferred that the TSF sends a fatal error alert message (e.g., unexpected message) in response to this, but it is acceptable that the TSF terminates the connection silently (i.e., without sending a fatal error alert).

{/old}

shall be replaced by

{new}

Test 4a [conditional, if the TOE supports TLS 1.3]: The evaluator shall initiate a TLS session between the TSF and a test TLS 1.3 server that completes a compliant TLS 1.3 handshake, followed by a hello request message. The evaluator shall observe that the TSF completes the initial TLS 1.3 handshake successfully, but terminates the session on receiving the hello request message.

It is preferred that the TSF sends a fatal error alert message (e.g., unexpected message) in response to this, but it is acceptable that the TSF terminates the connection silently (i.e., without sending a fatal error alert).

Test 4b [conditional, if the TOE supports TLS 1.2 and rejects TLS 1.2 renegotiation attempts]: The evaluator shall initiate a TLS session between the so configured TSF and a test TLS 1.2 server that is configured to perform a compliant handshake, followed by a hello request. The evaluator shall confirm

that the TSF completes the initial handshake successfully but does not initiate renegotiation after receiving the hello request.

{/new}.

Rationale:

see Issue section

Further Action:

None

Action by Network iTC:

None