Network Device Interpretation # 201828rev2

Different handling of TLS1.1 and TLS1.2 in Test 2 of FCS_TLSS_EXT.2.4+2.5

Status: ☒ *Active* ☐ *Inactive*

Date: *6-Mar-2019*

End of proposed Transition Period (to be updated after TR2TD process): *6-Mar-2019*

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): *ND SD v2.0e, ND SD v2.1*

Affected Section(s): *FCS_TLSS_EXT.2.4+2.5*

Superseded Interpretation(s): *Rfl#201828(rev1)*

Issue:

FCS_TLSS_EXT2.4+2.5, Test 2 is currently worded as follows:

"Test 2: The evaluator shall configure the server to send a certificate request to the client without the supported_signature_algorithm used by the client's certificate. The evaluator shall attempt a connection using the client certificate and verify that the connection is denied."

This test is asking for the server to send a "certificate request" (which is a major item in TLS. See section 7.4.4 of RFC5246 and RFC4346, section 5.5 of RFC4492) to the client without the "supported signature algorithm" (which is a defined item in section 7.4.4 of RFC5246, but NOT RFC4346) used by the client's certificate. So it's asking for the server's message to contain a list of supported signature algorithms. Section 7.4.4 of RFC 5246 (TLS 1.2) includes a supported_signature_algorithms field. The value represents the list of the hash/signature algorithm pairs that the server is able to verify. This field is new in TLS 1.2 and does not exist in older versions, so it is not included in RFC 4346 and therefore doesn't apply to TLS 1.1.

Therefore, Test 2 should be conditional based on the version of TLS selected.

<u>Proposed resolution:</u>

"Test 2[conditional]: If TLS1.2 is supported by the TOE, the evaluator shall configure the server to send a certificate request to the client without the supported_signature_algorithm used by the client's certificate. The evaluator shall attempt a connection using the client certificate and verify that the connection is denied."

Resolution:

The NIT acknowledges the issue described in the 'Issue' section. Therefore the following changes shall be performed:

FCS_TLSS_EXT2.4+2.5, Test 2 shall be modified as follows:

<old>"Test 2: The evaluator shall configure the server to send a certificate request to the client without the supported_signature_algorithm used by the client's certificate. The evaluator shall attempt a connection using the client certificate and verify that the connection is denied."</old>

shall be changed to

<new>"Test 2[conditional]: If TLS1.2 is claimed for the TOE, the evaluator shall configure the server to send a certificate request to the client without the supported_signature_algorithm used by the client's certificate. The evaluator shall attempt a connection using the client certificate and verify that the connection is denied."</new>

Rationale:

See 'Issue' section.

Further Action:

None

Action by Network iTC:

None