Network Device Interpretation # 201901

Using 'diffie-hellman-group-exchange-sha256' in FCS_SSHC/S_EXT.1.7

Status: ☒ *Active* □ *Inactive*

Date: *4-Jun-2019*

End of proposed Transition Period (to be updated after TR2TD process): *4-Jun-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): *NDcPP V2.0e, FWcPP V2.0e, NDcPP V2.1*

Affected Section(s): FCS_SSHC_EXT.1.7, FCS_SSHS_EXT.1.7

Superseded Interpretation(s): *None*

Issue:

FCS_SSHC_EXT.1.7, FCS_SSHS_EXT.1.7 allow selection of 'diffie-hellman-group14-sha256' for key exchange. The 'diffie-hellman-group14-sha256' is defined in more recent RFC 8228. Popular SSH packages such as OpenSSH have not yet implemented this selection. However, they do have another SSH method which achieves the same outcome. RFC 4419 defines 'diffie-hellman-group-exchange-sha256'. When 'diffie-hellman-group-exchange-sha256' is communicated to peer, it is followed by group negotiation handshake. If DH group 14 is the only one that is installed in TOE, the group negotiation results into agreement to use DH group 14. Thus the effective scheme becomes 'diffie-hellman-group14-sha256 '.

Please advise if it is possible to select 'diffie-hellman-group14-sha256' in SFR selection and implement it using combination of 'diffie-hellman-group-exchange-sha256' followed by DH group 14 group negotiation as outlined above.

Resolution:

The NIT understands that in case an open key exchange group is used which is then restricted to a specific cipher, the TOE would behave like a TOE where a specific key exchange group is implemented. But the restriction to acceptable key exchange groups is dependent on proper configuration of the TOE. From the NIT's perspective the correct configuration would need to be tested to avoid the use of weak key exchange groups due to misconfiguration. The related supporting Documents (i.e. ND SD V2.0e and ND SD V2.1) do not foresee such testing. Since NDcPP requires exact conformance and the ND SD does not provide sufficient evaluation activities for the proposed approach, the NIT is of the opinion that the proposed approach is not suitable to fulfill the requirements in FCS_SSHC_EXT.1.7/FCS_SSHS_EXT.1.7.

Rationale:

See resolution section.

Further Action:

None.

Action by Network iTC:

The Network iTC should consider to add necessary testing activities in a future version of the ND SD to support the option of an open key exchange group as described in the Issue section.