Network Device Interpretation # 201817

FCS_SSH*_EXT.1.1 RFCs for AES-CTR

Status: ☒ *Active* □ *Inactive*

Date: *23-Oct-2018*

End of proposed Transition Period (to be updated after TR2TD process): *23-Nov-2018*

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): *NDcPPv2.0E, FWcPPv2.0E, NDcPP V2.1*

Affected Section(s): *FCS_SSHC_EXT.1.1, FCS_SSHS_EXT.1.1*

Superseded Interpretation(s): *None*

Issue:

Issue:

NDcPPv2.0

*FCS_SSH*_EXT.1.1 provides a list of RFCs to which the TOE may claim conformance; however, this list does not contain an RFC specifying AES-CTR as allowed by FCS_SSH*_EXT.1.4.*

Proposed Resolution:

*Recommendation: Update the FCS_SSH*_EXT.1.1 to include RFC 4344.*

*In a future update, we recommend updating FCS_SSH*_EXT.1 to keep the core SSH RFCs (4251, 4252, 4253, 4254) and add algorithm specific RFC references to the various cryptographic selections within the subsequent elements similar to other cryptographic protocols (e.g. aes128-ctr, as specified by RFC4344.*

Resolution:

The NIT acknowledges the issue described in the 'Issue' section above. To resolve this the following changes shall be performed:

NDcPPv2.0E, FWcPPv2.0E FCS_SSHC_EXT.1 and FCS_SSHS_EXT.1 SFR shall be modified as follows:

*<old>"FCS_SSH*_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) [selection: 4251, 4252, 4253, 4254, 5647, 5656, 6187, 6668]."</old>*

shall be replaced by

*<new>"FCS_SSH*_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) [selection: 4251, 4252, 4253, 4254, 4344, 5647, 5656, 6187, 6668]."</new>*

<u>NDcPPv2.1, FCS_SSHC_EXT.1 and FCS_SSHS_EXT.1 SFR shall be modified as follows:</u>

*<old>"FCS_SSH*_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) [selection: 4251, 4252, 4253, 4254, 5647, 5656, 6187, 6668, 8332]."</old>*

shall be replaced by

*<new>"FCS_SSH*_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFC(s) [selection: 4251, 4252, 4253, 4254, 4344, 5647, 5656, 6187, 6668, 8332]."</new>*

<u>NDcPPv2.0E FCS_SSHC_EXT.1 and FCS_SSHS_EXT.1 Application Note 90 and 97 shall be modified as follows:</u>

The following paragraphs shall be added to the application notes:

<new>

*If claiming aes128-ctr or aes256-ctr encryption methods as part of FCS_SSH*_EXT.1.4 select RFC 4344. If claiming AEAD_AES_128_GCM or AEAD_AES_256_GCM (but not @openssh variants) encryption methods as part of FCS_SSH*_EXT.1.4 select RFC 5647.*

*If claiming ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, or ecdsa-sha2-nistp521 public key algorithms as part of FCS_SSH*_EXT.1.5 select RFC 5656. If claiming ecdh-sha2-nistp256, ecdh-sha2-nistp384, or ecdh-sha2-nistp521 key exchange methods as part of FCS_SSH*_EXT.1.7 select RFC 5656.*

*If claiming x509v3_* public key authentication as part of FCS_SSH*_EXT.1.5 select RFC 6187.*

*If claiming hmac-sha2-256 or hmac-sha2-512 algorithms as part of FCS_SSH*_EXT.1.6 select RFC 6668. If claiming hmac-sha1 or hmac-sha1-96 algorithms as part of FCS_SSH*_EXT.1.6 claim RFC 4253.*

Future versions of this cPP will include additional key exchange algorithms specified in RFC 8268 and additional RSA-based public key algorithms specified in RFC 8332.

</new>

<u>NDcPPv2.1 FCS_SSHC_EXT.1 and FCS_SSHS_EXT.1 Application Note 94 and 101 shall be modified as follows:</u>

The following paragraphs shall be added to the application notes:

<new>

*If claiming aes128-ctr or aes256-ctr encryption methods as part of FCS_SSH*_EXT.1.4 select RFC 4344. If claiming AEAD_AES_128_GCM or AEAD_AES_256_GCM (but not @openssh variants) encryption methods as part of FCS_SSH*_EXT.1.4 select RFC 5647.*

*If claiming ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, or ecdsa-sha2-nistp521 public key algorithms as part of FCS_SSH*_EXT.1.5 select RFC 5656. If claiming ecdh-sha2-nistp256, ecdh-sha2-nistp384, or ecdh-sha2-nistp521 key exchange methods as part of FCS_SSH*_EXT.1.7 select RFC 5656.*

*If claiming x509v3_* public key authentication as part of FCS_SSH*_EXT.1.5 select RFC 6187.*

*If claiming hmac-sha2-256 or hmac-sha2-512 algorithms as part of FCS_SSH*_EXT.1.6 select RFC 6668. If claiming hmac-sha1 or hmac-sha1-96 algorithms as part of FCS_SSH*_EXT.1.6 claim RFC 4253.*

Future versions of this cPP will include additional key exchange algorithms specified in RFC 8268.

</new>

Rationale:

As stated in the resolution section

Further Action:

Update cPP to include additional key exchange algorithms specified in RFC 8268.

Action by Network iTC:

None