Network Device Interpretation # 201908

NDcPP v2.1 Clarification - FCS_SSHC/S_EXT1.5

Status: ☒ *Active* □ *Inactive*

Date: *20-May-2019*

End of proposed Transition Period (to be updated after TR2TD process): *20-May-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 V2.1*

Affected Section(s): FCS_SSHC_EXT.1.5, FCS_SSHS_EXT.1.5

Superseded Interpretation(s): *None*

Issue:

A vendor is entering in an evaluation that is claiming compliance to the collaborative Protection Profile for Network Devices Version 2.1. which includes the SFR FCS_SSHS_EXT.1 – SSH Server Protocol. The CCTL is requesting clarification on FCS_SSHS_EXT.1.5 and FCS_SSHC_EXT.1.5 as it is identified in the cNDPP v2.1.

The cNDPP identifies the SFR as:

"FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: ssh-rsa, **rsa-sha2-256, rsa-sha2-512**, ecdsa-sha2-nistp256, x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256] as its public key algorithm(s) and rejects all other public key algorithms."

The cNDPP Section 6.1 identifies the PP conventions as the following:

Selection wholly or partially completed in the PP: the selection values (i.e. the selection values adopted in the PP or the remaining selection values available for the ST) are indicated with underlined text

e.g. "[selection: disclosure, modification, loss of use]" in [CC2] or an ECD might become "disclosure" (completion) or "[selection: disclosure, modification]" (partial completion) in the PP;

Is it the PP authors intent to make "rsa-sha2-256, rsa-sha2-512" a mandatory selected component for FCS_SSHS_EXT.1.5 and FCS_SSHC_EXT.1.5?

Resolution:

The formatting of the SFRs FCS_SSHC_EXT.1.5 and FCS_SSHS_EXT.1.5 needs to be corrected as follows:

<old> The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: *ssh-rsa, **rsa-sha2-256, rsa-sha2-512,** ecdsa-sha2-nistp256, x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256*] as its public key algorithm(s) and rejects all other public key algorithms.</old>
Shall be reformatted to (without any change of the content)
<new> The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: *ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp256, x509v3-ssh-rsa, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256*] as its public key algorithm(s) and rejects all other public key algorithms.</new>

Rationale:

FCS_SSHC_EXT.1.5 and FCS_SSHS_EXT.1.5 properly replicate the SFR as defined in the ECD. The current formatting of the two ciphers in the ECD seems to be a mistake and need therefore to be corrected (Why would an option in a selection be marked as partially completed in the ECD?). The current formatting would not indicate, though, that the options would be mandatory as indicated by the originator of the RfI, since the formatting just indicates a refinement and a partially completed operation.

Further Action:

None.

Action by Network iTC:

None.