Network Device Interpretation # 201612rev2

Password authentication for SSH clients

Status: ☒ *Active* ☐ *Inactive*

Date: *21-Apr-2017*

Type of Document: ☒ *Technical Decision* ☐ *Technical Recommendation*

Approved by: ☒ *Network iTC Interpretations Team* ☐ *Network iTC*

Affected Document(s): *NDcPP V1.0, FWcPP V1.0*

Affected Section(s): *FCS_SSHC_EXT.1.2*

Superseded Interpretation(s): *RfI#(2016)12, 15-Feb-2016*

Issue:

NDcPP V1.0: FCS_SSHC_EXT.1.2 requires an SSH client to support both password and public key authentication. It seems like a TOE would usually be an SSH client when using SSH to establish a trusted channel with an IT entity where public key authentication would normally be used. Can password based authentication be made optional?

Resolution:

The NIT acknowledges the issue described in the 'Issue' section above. FCS_SSHC_EXT.1.2 shall therefore be modified as follows:

FCS_SSHC_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: password-based, no other method].

The TSS section in the Supporting Document for FCS_SSHC_EXT.1.2 shall be replaced by the following:

The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication and that this list conforms to FCS_SSHC_EXT.1.5. and ensure that if password-based authentication methods have been selected in the ST then these are also described.

Test 1 in the Tests section in the Supporting Document for FCS_SSHC_EXT.1.2 remains unchanged.

Test 2 in the Tests section in the Supporting Document for FCS_SSHC_EXT.1.2 shall be replaced by the following:

Test 2: This test is only applicable if password-based authentication has been selected in FCS_SSHC_EXT.1.2 in the ST. Otherwise this test shall be omitted. Using the guidance documentation, the evaluator shall configure the TOE to perform password-based authentication to an SSH server, and demonstrate that a user can be successfully authenticated by the TOE to an SSH server using a password as an authenticator.

Rationale:

The decision is in agreement with RFC 4252, chap. 5.

Further Action:

None.

Action by Network iTC: