Network Device Interpretation # 201728

Selections in FCS_SSH*_EXT.1.6

Status: ☒ *Active* ☐ *Inactive*

Date: *1-Aug-2018*

End of proposed Transition Period (to be updated after TR2TD process): *1-Sep-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): *NDcPP v2.0e, FWcPP v2.0e, ND SD v2.0e*

Affected Section(s): *FCS_SSHC_EXT.1, FCS_SSHS_EXT.1*

Superseded Interpretation(s): *None*

Issue:

FCS_SSH*_EXT.1.6 does not allow the solitary selection of AEAD_AES_128_GCM and/or AEAD_AES_256_GCM for the MAC algorithm. The requirement also mandates the ST author also make a selection of hmac-sha1, hmac-sha1-96, hmac-sha2-256 and/or hmac-sha2-512 as the MAC algorithm.

As described in RFC 5647 and Application Notes 92/99, when AEAD_AES_128_GCM and/or AEAD_AES_256_GCM are selected as the encryption algorithm(s), it must also be selected as the MAC algorithm(s). AEAD_AES_128_GCM and/or AEAD_AES_256_GCM provides for both encryption and integrity.

It should be noted that FCS_SSH*_EXT.1.4 does allow the solitary selections of AEAD_AES_128_GCM, and/or AEAD_AES_256_GCM as the encryption algorithm(s).

Test 2 requires the evaluator to configure an SSH server/client to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the TOE to the SSH server/client and observe that the attempt fails.

Test 2 is not an appropriate test when AEAD_AES_128_GCM, and/or AEAD_AES_256_GCM is selected since it provides for both encryption and integrity. When the evaluator tests with a MAC algorithm such as HMAC-MD5, the connection is successful because the HMAC is ignored.

<u>Proposed Resolution:</u>

Combine the selection operations in FCS_SSH*_EXT.1.6 as follows:

FCS_SSH*_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [selection: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512, AEAD_AES_128_GCM, AEAD_AES_256_GCM] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

Designate Test 2 in the requirement as "Conditional" and applicable only if HMAC is selected as the MAC algorithm(s)

Resolution:

The NIT acknowledges the issue described in the 'Issue' section.

NDcPP V2.0e, FWcPP V2.0e, FCS_SSHC_EXT.1.1 and FCS_SSHS_EXT.1.1

The following shall be added to Application Notes 90 and 97:

> *RFC 5647 only applies to the RFC compliant implementation of GCM; a TOE that only implements the "@openssh.com" variant of GCM should not select 5647. aes*-gcm@openssh.com is specified in* Section 1.6 of *the OpenSSH Protocol Specification (https://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/PROTOCOL?rev=1.31).*

NDcPP V2.0e, FWcPP V2.0e, FCS_SSHC_EXT.1.4 and FCS_SSHS_EXT.1.4

The SFR element shall be modified to as follows:

> <old>The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: *[selection: aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr, AEAD_AES_128_GCM, AEAD_AES_256_GCM]*.</old>
>
> <new>The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: *[selection: aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr, AEAD_AES_128_GCM, AEAD_AES_256_GCM, aes128-gcm@openssh.com, aes256-gcm@openssh.com]*.</new>

NDcPP V2.0e, FWcPP V2.0e, FCS_SSHC_EXT.1.6 and FCS_SSHS_EXT.1.6

The SFR element shall be modified to as follows:

> <old>The TSF shall ensure that the SSH transport implementation uses *[selection: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512] and [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other MAC algorithms]* as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).</old>
>
> <new>The TSF shall ensure that the SSH transport implementation uses *[selection: hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512, AEAD_AES_128_GCM, AEAD_AES_256_GCM, implicit]* as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).</new>

The following shall be appended to Application Notes 94 and 101:

> *The ST author selects "implicit" when, and only when, aes*-gcm@openssh.com is selected as an encryption algorithm. When aes*-gcm@openssh.com is negotiated as the encryption algorithm,*

the MAC algorithm field is ignored and GCM is implicitly used as the MAC. "implicit" is not an SSH algorithm identifier and will not be seen on the wire; however, the negotiated MAC might be decoded as "implicit".

ND SD V2.0e, FCS_SSHC_EXT.1.6

The text for the Tests shall be modified as follows:

> Test 1: (conditional, if an HMAC or AEAD_AES_*_GCM algorithm is selected in the ST) The evaluator shall establish an SSH connection using each of the algorithms, except "implicit", specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.
>
> Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
>
> Test 2: (conditional, if an HMAC or AEAD_AES_*_GCM algorithm is selected in the ST) The evaluator shall configure an SSH server to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the TOE to the SSH server and observe that the attempt fails.
>
> Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.

ND SD V2.0e, FCS_SSHS_EXT.1.6

The text for the Tests shall be modified as follows:

> Test 1: (conditional, if an HMAC or AEAD_AES_*_GCM algorithm is selected in the ST) The evaluator shall establish an SSH connection using each of the algorithms, except "implicit", specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.
>
> Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
>
> Test 2: (conditional, if an HMAC or AEAD_AES_*_GCM algorithm is selected in the ST) The evaluator shall configure an SSH client to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.
>
> Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.

Rationale:

The key exchange defined for AES GCM defined in Section 5.1 of RFC 5467 is ambiguous regarding how the encryption and MAC algorithm should be negotiated. To resolve this ambiguity, a de facto standard has emerged whereby if AES GCM is negotiated as the encryption algorithm by use of aes-gcm@openssh.com, the MAC field is ignored. (https://cvsweb.openbsd.org/cgi-*

bin/cvsweb/src/usr.bin/ssh/PROTOCOL?rev=1.31 section 1.6). This RFI aligns the MAC testing assurance activities with this behavior.

Further Action:

None

Action by Network iTC:

None