Network Device Interpretation # 201824

Separate traffic consideration for SSH rekey

Status: ☒ *Active* □ *Inactive*

Date: *11-Dec-2018*

End of proposed Transition Period (to be updated after TR2TD process): *11-Jan-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): *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Superseded Interpretation(s): *None.*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:

*FCS_SSH*_EXT.1.8 was modified by TD0167/ NIT interpretation #201624 to change the SFRs and assurance activities.*

The SFRs now read, "The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed."

Since not all data in an SSH connection is encrypted (e.g. GCM tag, GCM AAD), this should be based on the data encrypted using a single key. There is no need to rekey based on data that has not been encrypted.

The test includes the following statement, "The transmitted traffic is the total traffic comprising incoming and outgoing traffic."

We have the following concerns with this test:

1. SSH generates independent keys for sending and receiving data, so it does not make sense to rekey based on the combined total.

2. As with the SFR, this is based on transmitted traffic and not data encrypted with a specific key.

3. Standard open source implementations of SSH (i.e. OpenSSH) cannot be configured to rekey based on total data encrypted without modification of the implementation.

We recommend updating the SFR to read:

The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

We recommend updating the “For testing of the traffic-based threshold” paragraphs to read:

“…shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. The evaluator shall verify the test [client/server] does not initiate the rekey.”

Resolution:

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

FCS_SSHC_EXT.1.8 and FCS_SSHS_EXT.1.8 shall be modified as follows:

*<old>"*The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed."</old>

shall be replaced by

<new>" The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed."*</new>*

The first paragraph of the Application Note for FCS_SSHC_EXT.1.8 and FCS_SSHS_EXT.1.8 shall be modified as follows:

*<old>"*This SFR defines two thresholds - one for the maximum time span the same session keys can be used and the other one for the maximum amount of data that can be transmitted using the same session keys. Both thresholds need to be implemented and a rekey needs to be performed on whichever threshold is reached first. For the maximum transmitted data threshold, total incoming and outgoing data needs to be counted. The rekey applies to all session keys (encryption, integrity protection) for incoming and outgoing traffic."*</old>*

shall be replaced by

<new>" This SFR defines two thresholds - one for the maximum time span the same session keys can be used and the other one for the maximum amount of data that can be transmitted using the same session keys. Both thresholds need to be implemented and a rekey needs to be performed on whichever threshold is reached first. For the maximum transmitted data threshold, the encrypted traffic per encryption key needs to be counted. It is also acceptable to count the totally transmitted data per encryption key, the total encrypted traffic for incoming and outgoing data or the total transmitted incoming and outgoing data because the encrypted traffic per encryption key will always be lower or equal to the other options. The rekey requirement applies to all session keys (encryption, integrity protection) for incoming and outgoing traffic."*</new>*

The fourth paragraph in the test description for FCS_SSHC_EXT.1.8 shall be modified as follows:

*<old>"*For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH server, and shall transmit data from and to the TOE within the active SSH session until the threshold for transmitted traffic is reached. The transmitted traffic is the total traffic comprising incoming and outgoing traffic.*"</old>*

shall be replaced by

*<new>"*For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH server, and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHC_EXT.1.8). *"</new>*

The fourth paragraph in the test description for FCS_SSHS_EXT.1.8 shall be modified as follows:

*<old>"*For testing of the traffic-based threshold the evaluator shall use an SSH client to connect to the TOE, and shall transmit data from and to the TOE within the active SSH session until the threshold for transmitted traffic is reached. The transmitted traffic is the total traffic comprising incoming and outgoing traffic.*"</old>*

shall be replaced by

*<new>"*For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH client, and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHS_EXT.1.8). *"</new>*

Rationale:

As stated in the resolution section.

RfI#201624 mandated counting of the total incoming and outgoing traffic. This decision was based on the fact that the encryption keys are derived from the same keying material provided during the key exchange*. Triggered by RfI#201824 a more detailed analysis has been performed and based on that it has been regarded as unlikely to derive one key from the other with reasonable effort.*

Further Action:

None

Action by Network iTC:

None