Network Device Interpretation # 201814

Audit requirements for FCS_SSH*_EXT.1.8

Status: ☒ *Active* ☐ *Inactive*

Date: *18-Jul-2018*

End of proposed Transition Period (to be updated after TR2TD process): *18-Jul-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): *ND SD v2.0e*

Affected Section(s): *FCS_SSHC_EXT.1.8, FCS_SSHS_EXT.1.8*

Superseded Interpretation(s): *None*

Issue:

The SD for collaborative network device protection profile version 2.0 states "For testing of the time-based threshold the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and a corresponding audit event has been generated by the TOE" for both SSHS_EXT.1.8 and SSHC_EXT.1.8. NIAP TD0150 removes the SSH rekey audit from FAU_GEN.1 in CPP_ND_V1.0 which appears to have remained persistent with CPP_ND_V2.0.

The lab believes the audit should also be removed from the SD for NDcPP, version 2.0.

Resolution:

The NIT acknowledges the issue described in the 'Issue' section. Therefore the following changes shall be applied.

The second paragraph of the test section for FCS_SSHC_EXT.1.8 shall be modified as follows:

> <old>"For testing of the time-based threshold the evaluator shall use the TOE to connect to an SSH server and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and a corresponding audit event has been generated by the TOE."</old>

shall be replaced by

<new>"For testing of the time-based threshold the evaluator shall use the TOE to connect to an SSH server and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator)."</new>

The fifth paragraph of the test section for FCS_SSHC_EXT.1.8 shall be modified as follows:

<old>"The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and a corresponding audit event has been generated by the TOE."</old>

shall be replaced by

<new>" The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator)."</new>

The second paragraph of the test section for FCS_SSHS_EXT.1.8 shall be modified as follows:

<old>"For testing of the time-based threshold the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and a corresponding audit event has been generated by the TOE."</old>

shall be replaced by

<new>"For testing of the time-based threshold the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator)."</new>

The fifth paragraph of the test section for FCS_SSHS_EXT.1.8 shall be modified as follows:

<old>"The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and a corresponding audit event has been generated by the TOE."</old>

shall be replaced by

<new>"The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator)."</new>

Rationale:

see 'Issue' section

Further Action:

None

Action by Network iTC:

None