Network Device Interpretation # 201641

Removal of SSH re-key audit events

Status: ☒ *Active* ☐ *Inactive*

Date: *19-Jan-2017*

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

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

Affected Document(s): *ND cPP V1.0, FW cPP V1.0*

Affected Section(s): *FAU_GEN.1*

Superseded Interpretation(s): *None*

Issue:

The NIAP technical decision TD0082 allows for the removal of the SSH Rekeying from FAU_GEN.1 auditable events in the Mobile Device Management PP (PP_MDM_V2.0).

https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=85

“Resolution

In Table 1, "Successful SSH re-key." should be removed from the Auditable Events column for FCS_SSHS_EXT.1.

Justification

This level of auditing is not deemed necessary, and the most popular SSH implementation does not support it. “”

Would it be correct to apply this technical decision to the collaborative Protection Profile for Network Devices (CPP_ND_V1.0)?

Resolution:

The NIT agrees with the Resolution and Justification provided in NIAP TD0082.

FAU_GEN.1, Table 4 shall therefore be changed as follows:

'Successful SSH rekey' shall be removed from Table 4 as auditable events for FCS_SSHC_EXT.1 and FCS_SSHS_EXT.1.

Rationale:

Auditing of re-key events is regarded as debug level information rather than auditing of regular security audit events and can therefore be omitted.

Further Action:

None

Action by Network iTC:

None