Network Device Interpretation # 202411

Correction of FCS_IPSEC_EXT.1.4, Evaluation Activities/App Note

Status: ☒ *Active* ☐ *Inactive*

Date: *15-Jul-2024*

End of proposed Transition Period (to be updated after TR2TD process): *15-Aug-2024*

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): *NDSD v3.0e*

Affected Section(s): *FCS_IPSEC_EXT.1.4*

Superseded Interpretation(s): *None*

Issue:

Issue:

Would it be possible to add an additional Evaluation Activity and Application Note for FCS_IPSEC_EXT.1.4 to ensure that when AES-CBC is claimed that the claimed HMAC algorithm's security strengths is ≥ 192 or ≥ the security strength of the AES key and the security strength and algorithm is supported by the DRBG (e.g., FCS_RBG_EXT.1.1)?

My understanding is that when multiple algorithms are used together the security strength is determined by the weakest level of security provided from the protections. The below example could be problematic and confusing for administrators, auditors, etc.

For example, for VID 11333, for FCS_IPSEC_EXT.1.4, AES-CBC-256 with HMAC-SHA-1 was claimed, which I believe would result in a security strength of 128 instead of the intended 256.

Resolution:

The NIT disagrees with the proposed change, because confidentiality and integrity requirements of a TOE might be independent; tying them together could prevent certain useful implementations.

There is no need for the confidentiality and integrity to have the same security strengths, and in many situations, users may have a need for one service to be stronger than the other, especially if the protection of one service is needed for a much longer time than the other service (e.g. short-term integrity protection during transfer vs. long-term protection of confidentiality).

Rationale:

see Resolution section

Further Action:

None

Action by Network iTC:

None