Network Device Interpretation # 202406

Applying TD0800 to NDcPP v3.0E

Status: ☐ *Active* ☒ *Inactive*

Date: *10-Jul-2024*

End of proposed Transition Period (to be updated after TR2TD process): *10-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): *NDcPP v3.0e*

Affected Section(s): *FCS_IPSEC_EXT.1.7, FCS_IPSEC_EXT.1.8*

Superseded Interpretation(s): *None*

Issue:

Issue:

The CCTL observed that TD0800, which allows for configuration of shorter SA lifetimes than the maximum 24 (IPSEC_EXT.1.7)/8 (IPSEC_EXT.1.8) hours was not applied to NDcPP v3.0E. It is assumed that this is because the newer PP was already in the finalization process when the TD was issued. The CCTL requests clarification as to whether the absence of these materials from NDcPP v3.0E is intentional or if this should also be applied to the newer version of the PP as well.

Resolution:

The NIT acknowledges the issue. The following change shall be applied to Section B.3.1.3 of the cPP:

{old}

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [selection:

- *IKEv1 Phase 1 SA lifetimes can be configured by a Security Administrator based on* [selection:
  - *number of bytes;*
  - *length of time, where the time values can be configured within [assignment: integer range including 24] hours;*

];

- *IKEv2 SA lifetimes can be configured by a Security Administrator based on*

[selection:

- *number of bytes;*
- *length of time, where the time values can be configured within [assignment: integer range including 24] hours]*

].

Application Note 88

The ST author chooses either the IKEv1 requirements or IKEv2 requirements (or both, depending on the selection in FCS_IPSEC_EXT.1.5). The ST author chooses either volume-based lifetimes or time-based lifetimes (or a combination). This requirement must be accomplished by providing Security Administrator-configurable lifetimes (with appropriate instructions in documents mandated by AGD_OPE). Hardcoded limits do not meet this requirement. In general, instructions for setting the parameters of the implementation, including lifetime of the SAs, should be included in the guidance documentation generated for AGD_OPE.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection:

- *IKEv1 Phase 2 SA lifetimes can be configured by a Security Administrator based on* [selection:
  - *number of bytes;*
  - *length of time, where the time values can be configured within [assignment: integer range including 8] hours;*

];

- *IKEv2 Child SA lifetimes can be configured by a Security Administrator based on* [selection:
  - *number of bytes;*
  - *length of time, where the time values can be configured within [assignment: integer range including 8] hours;*

].

Application Note 89

The ST author chooses either the IKEv1 requirements or IKEv2 requirements (or both, depending on the selection in FCS_IPSEC_EXT.1.5). The ST author chooses either volume-based lifetimes or time-based lifetimes (or a combination). This requirement must be accomplished by providing Security Administrator-configurable lifetimes (with appropriate instructions in documents mandated by AGD_OPE). Hardcoded limits do not meet this requirement. In general, instructions for setting the parameters of the implementation, including lifetime of the SAs, should be included in the guidance documentation generated for AGD_OPE.

{/old}

shall be replaced by

{new}

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [selection:

- *IKEv1 Phase 1 SA lifetimes can be configured by a Security Administrator based on* [selection:
    - *number of bytes;*
    - *length of time, where the time values can be configured between [assignment: minimum configurable rekey time] and [assignment: maximum configurable rekey time];*

  ];
- *IKEv2 SA lifetimes can be configured by a Security Administrator based on* [selection:
    - *number of bytes;*
    - *length of time, where the time values can be configured between [assignment: minimum configurable rekey time] and [assignment: maximum configurable rekey time]*

  ]

].

Application Note 88

The ST author chooses either the IKEv1 requirements or IKEv2 requirements (or both, depending on the selection in FCS_IPSEC_EXT.1.5). The ST author chooses either volume-based lifetimes or time-based lifetimes (or a combination). The range between the minimum and maximum rekeys time must be include a rekey time that causes a rekey to occur at or slightly before 24 hours. The exact values supported may vary by TOE implementation. Some TOEs might require the administrators to ensure rekeying prior to the desired time (e.g., configure a time value of 23h 59min to ensure the actual rekey is performed no later than 24h, while other TOEs might automatically ensure rekeying is performed prior to the configured time.

This requirement must be accomplished by providing Security Administrator-configurable lifetimes. Hardcoded limits do not meet this requirement.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [selection:

- *IKEv1 Phase 2 SA lifetimes can be configured by a Security Administrator based on* [selection:
    - *number of bytes;*
    - *length of time, where the time values can be configured between [assignment: minimum configurable rekey time] and [assignment: maximum configurable rekey time];*

  ];
- *IKEv2 Child SA lifetimes can be configured by a Security Administrator based on* [selection:
    - *number of bytes;*
    - *length of time, where the time values can be configured between [assignment: minimum configurable rekey time] and [assignment: maximum configurable rekey time];*

  ]

].

Application Note 89

The ST author chooses either the IKEv1 requirements or IKEv2 requirements (or both, depending on the selection in FCS_IPSEC_EXT.1.5). The ST author chooses either volume-based lifetimes or time-based lifetimes (or a combination). The range between the minimum and maximum rekeys time must be include a rekey time that causes a rekey to occur at or slightly before 8 hours. The exact values

supported may vary by TOE implementation. Some TOEs might require the administrators to ensure rekeying prior to the desired time (e.g., configure a time value of 7h 59min to ensure the actual rekey is performed no later than 8h, while other TOEs might automatically ensure rekeying is performed prior to the configured time.

This requirement must be accomplished by providing Security Administrator-configurable lifetimes. Hardcoded limits do not meet this requirement.

{/new}.

Rationale:

see Issue section

Further Action:

None

Action by Network iTC:

None