Network Device Interpretation # 201907rev4

Missing EAs for FCS_NTP_EXT.1.4

Status: ☒ *Active* ☐ *Inactive*

Date: *15-May-2020*

End of proposed Transition Period (to be updated after TR2TD process): *15-May-2020*

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 v2.1, ND SD v2.2*

Affected Section(s): *FCS_NTP_EXT.1.4*

Superseded Interpretation(s): *RfI#201907rev3*

Issue:

NDcPP V2.1 has introduced a new SFR: FCS_NTP_EXT.1. The element FCS_NTP_EXT.1.4 requires a specific TOE capability, to "support configuration of at least 3 time sources". The Supporting Document for NDcPP v2.1 has no specific Assurance Activity regarding the ability of the TOE to support "configuration of at least three (3) NTP time sources".

In addition, in ND SD v2.2, instead of specifying two tests for FCS_NTP_EXT.1.4, one test has been specified for FCS_NTP_EXT.1.4 and one for FCS_NTP_EXT.1.5 by mistake, although FCS_NTP_EXT.1.5 is not defined in NDcPPV2.2.

Resolution:

The FCS_NTP_EXT.1 requirements have been developed by the NTP WG of the Network iTC. Together with the SFRs also the evaluation activities have been developed. It seems like the tests for FCS_NTP_EXT.1.4 got lost in the editorial process when NDcPP V2.1 and ND SD V2.1 have been drafted. Therefore, the following text shall be added to Tests section for FCS_NTP_EXT.1 in ND SD:

<new>

FCS_NTP_EXT.1.4

Test 1: The evaluator shall confirm the TOE supports configuration of at least three (3) NTP time sources. The evaluator shall configure at least three NTP servers to support periodic time updates to the TOE. The evaluator shall confirm the TOE is configured to accept NTP packets that would result in the timestamp being updated from each of the NTP servers. The evaluator shall check that the time stamp is *updated after receipt of the NTP packets. The purpose of this test to verify that the TOE can be configured to synchronize with multiple NTP servers. It is up to the evaluator to determine that the multi-source update of the time information is appropriate and consistent with the behaviour prescribed by the RFC 1305 for NTPv3 and RFC 5905 for NTPv4.*

Test 2: (The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers).

The evaluator shall confirm that the TOE would not synchronize to other, not explicitly configured time sources by sending an otherwise valid but unsolicited NTP Server responses indicating different time from the TOE's current system time. This rogue time source needs to be configured in a way (e.g. degrade or disable valid and configured NTP servers) that could plausibly result in unsolicited updates becoming a preferred time source if they are not discarded by the TOE. The TOE is not mandated to respond in a detectable way or audit the occurrence of such unsolicited updates. The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers. It is up to to the evaluator to craft and transmit unsolicited updates in a way that would be consistent with the behaviour of a correctly-functioning NTP server.

</new>

For ND SD V2.2 the tests specified for FCS_NTP_EXT.1.4 and FCS_NTP_EXT.1.5 shall be replaced as follows:

<old>

FCS_NTP_EXT.1.4

The evaluator shall confirm the TOE supports configuration of at least three (3) NTP time sources. The evaluator shall configure at least three NTP servers to support periodic time updates to the TOE. The evaluator shall confirm the TOE is configured to accept NTP packets that would result in the timestamp being updated from each of the NTP servers. The evaluator shall check that the time stamp is updated after receipt of the NTP packets.

FCS_NTP_EXT.1.5

The evaluator shall also confirm that the TOE does not synchronize to any other time sources by configuring another NTP source operating in the server mode and inducing (e.g. send synch request with a forged source IP address) it to send timestamp updates to the TOE. The evaluator shall check that the TSF does not act on the received NTP updates and does not update system time. The evaluator shall confirm that the time stamp is not updated for a valid reason (e.g. failure to recognize NTP authentication key or rejection of unrequested NTP synchronization).

</old>

shall be replaced by

<new>

FCS_NTP_EXT.1.4

Test 1: The evaluator shall confirm the TOE supports configuration of at least three (3) NTP time sources. The evaluator shall configure at least three NTP servers to support periodic time updates to the TOE. The evaluator shall confirm the TOE is configured to accept NTP packets that would result in the timestamp being updated from each of the NTP servers. The evaluator shall check that the time stamp is updated after receipt of the NTP packets. The purpose of this test to verify that the TOE can be configured to synchronize with multiple NTP servers. It is up to the evaluator to determine that the multi-source update of the time information is appropriate and consistent with the behaviour prescribed by the RFC 1305 for NTPv3 and RFC 5905 for NTPv4.

Test 2: (The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers).

The evaluator shall confirm that the TOE would not synchronize to other, not explicitly configured time sources by sending an otherwise valid but unsolicited NTP Server responses indicating different time from the TOE's current system time. This rogue time source needs to be configured in a way (e.g. degrade or disable valid and configured NTP servers) that could plausibly result in unsolicited updates becoming a preferred time source if they are not discarded by the TOE. The TOE is not mandated to respond in a detectable way or audit the occurrence of such unsolicited updates. The intent of this test is to ensure that the TOE would only accept NTP updates from configured NTP Servers. It is up to the evaluator to craft and transmit unsolicited updates in a way that would be consistent with the behaviour of a correctly-functioning NTP server.

</new>

Rationale:

See Issue section and resolution section.

Change from rev3 to rev4: Properly capture NDcPPv2.2 and move FCS_NTP_EXT.1.5 Test 1 to FCS_NTP_EXT.1.4 Test 2.

Further Action:

None

Action by Network iTC:

None