Network Device Interpretation # 202412

Test definition for FCS_NTP_EXT.1.2

Status: ☒ *Active* □ *Inactive*

Date: *9-Sep-2024*

End of proposed Transition Period (to be updated after TR2TD process): *9-Oct-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_NTP_EXT.1.2, Tests*

Superseded Interpretation(s): *None*

Issue:

Issue:

FCS_NTP_EXT.1.2 Second paragraph: "[conditional] If the message digest algorithm is claimed in element 1.2, the evaluator shall change the message digest algorithm used by the NTP server in such a way that the new value does not match the configuration on the TOE and confirms that the TOE does not synchronize to this time source."

The described test does not make a any sense and provides no assurance. As the TOE is always the NTP request initiator, this test if performed as written will just result in the NTP server rejecting/ignoring the request from the TOE, so the TOE does not receive NTP response and there is nothing to check here.

Proposed resolution:

This test needs to be removed or reworked.

One solution would be to reword it in a way that will require the evaluator to use a modified NTP server to send reply signed with the wrong digest. Another alternative would be to modify the test, prescribing the evaluator to corrupt the message digest.

e.g.: "[conditional] If the message digest algorithm is claimed in element 1.2, the evaluator shall initiate NTP requests from the TOE and ensure that the NTP response received by the TOE contains incorrect digest (digest algorithm does not match the configuration on the TOE or the digest value is modified in transit) and confirms that the TOE does not synchronize to this time source."

Resolution:

To overcome the issue described in the 'Issue' section the following changes shall be performed to the second paragraph of the test definition for FTP_NTP_EXT.1.2 in NDSDv3.0e:

{old}

[conditional] If the message digest algorithm is claimed in element 1.2, the evaluator shall change the message digest algorithm used by the NTP server in such a way that the new value does not match the configuration on the TOE and confirms that the TOE does not synchronize to this time source.

{/old}

shall be replaced by

{new}

[conditional] If the message digest algorithm is claimed in element 1.2, the evaluator shall configure the TOE and NTP server so the TOE can synchronize time using a claimed message digest algorithm. The evaluator shall modify the response(s) from the NTP server so the response(s) contains a MAC that was generated by a different message digest algorithm and confirm the TOE does not synchronize to this time source. Other than the invalid MAC, the NTP response(s) must be valid (e.g., key ID, key value used, timestamps).

Note: Since the algorithm is not identified in the server response, this tests an incorrect algorithm and an invalid MAC.

{/new}

Rationale:

From RFC 5905:

The MAC consists of the Key Identifier followed by the Message Digest. The message digest, or cryptosum, is calculated as in [RFC1321] over all NTP-header and optional extension fields, but not the MAC itself.

…

Additional checks are summarized in Figure 22. Note that all packets, including a crypto-NAK, are considered valid only if they survive these tests.

```
+--------------------------+----------------------------------------+
| Packet Type              | Description                            |
+--------------------------+----------------------------------------+
| 1 duplicate packet       | The packet is at best an old duplicate |
|                          | or at worst a replay by a hacker.      |
```

	This can happen in symmetric modes if the poll intervals are uneven.
2 bogus packet	
3 invalid	*One or more timestamp fields are invalid. This normally happens in symmetric modes when one peer sends the first packet to the other and before the other has received its first reply.*
4 access denied	*The access controls have blacklisted the source.*
5 authentication failure	*The cryptographic message digest does not match the MAC.*
6 unsynchronized	*The server is not synchronized to a valid source.*
7 bad header data	*One or more header fields are invalid.*

Figure 22: Packet Error Checks

The intent of the old conditional test is to validate the implementation of step #5 authentication failure in the NTP receive() routine and to confirm that if errors are found, the packet is discarded and the peer process exits.

Further Action:

None

Action by Network iTC:

None