Network Device Interpretation # 27

NDcPP FPT_TUD_EXT.1 TRRT Request - 2b

Status: ☒ *Active* ☐ *Inactive*

Date: *27-Jun-2016*

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): *FPT_TUD_EXT.1*

Superseded Interpretation(s): *None*

Issue:

2b. Furthering the discussion from question 2a., there may be difficulties with Test 2 - 2) and option (1). How an update package is assembled or delivered (direct download by TOE from a vendor's server) may make it difficult for the lab to ensure that the update does not contain a published hash. We understand that the lab can obtain an illegitimate update from the vendor but the lab would not directly know the reason that the update failed under scenario (1) was because the update did not have the hash value.

● *Is the lab expected to trust the vendor did not include the hash value in the update assuming the test was run and update fails?*

● *Other than informing the vendor that the TOE needs to use either SHA-1, SHA-256, SHA-384, or SHA-512 for hashing of the update, how can the lab confirm they are using the claimed method(s) for option (1) if only the vendor can produce the update package?*

Additionally, when the vendor uses a direct download mechanism for delivering updates posting an illegitimate update to their server could be harmful to their customer base. For most TOEs that we have worked on with direct download mechanisms there has been both an online (vendor's server) and offline (local server) method. It has previously been acceptable to validate an illegitimate update via only the offline method and we would expect this to still be the case.

● *We recommend including an application note in the PP stating this.*

● *Although we have not seen this to date, we recommend the Technical Community considers products that only have the online update method and what would need to be done to perform this test.*

Resolution:

Trusted Updates may not use a published hash without administrator intervention – See Also RFI#26 for further information and clarification.

A local server is sufficient for testing. Labs should work with vendors to define an appropriate update environment to best replicate and test the TOEs operational behavior. The official documentation will not be updated. This interpretation will serve as official notice.

Rationale:

RFI#26 explicitly disallows automatic installation for an update that solely uses published hashes.

The lab and vendor should work to determine an appropriate testing strategy that demonstrates the TOE's conformance to FPT_TUD_EXT.1. If operational behavior can be demonstrated in a non-production environment, that is sufficient.

Further Action:

None

Action by Network iTC:

None