HCD0004 - FDP_DSK_EXT.1 testing limited to data encryption performed by operating TSFI

Version: 1, Published: 2024-01-29

Impacted Documents

CPP_HCD_V1.0_supporting_doc

References

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

Issue Description

The TSF can encrypt data within the scope of FDP_DSK_EXT.1 without the operation of TSFI. The tests for FDP_DSK_EXT.1 do not include the validation of data encryption in which data is encrypted without the operation of TSFI.

Resolution

Add tests for FDP_DSK_EXT.1 for the case in which the TSF encrypts the data without the operation of TSFI.

CPP_HCD_V1.0_supporting_doc

The SD is updated as follows (yellow highlights for additions, strikethrough for deletions) per section that is being updated:

3.1.3.1. TSS

If any D.USER.DOC or D.TSF.CONF are transparently encrypted and written to disk via mechanisms other than operating TSFI, the evaluator shall verify that the TSS identifies those mechanisms and describes at a high level how the associated data are encrypted. The swap files and core dump may potentially contain D.USER.DOC or D.TSF.CONF should be considered.

3.1.3.4. Tests

Test 5. [Conditional: If any D.USER.DOC or D.TSF.CONF are transparently encrypted and written to disk via mechanisms other than operating TSFI] Using a special tooling that the developer shall

provide, the evaluator shall write the known data to the storage through transparent encryption.

Test 6. [Conditional: If any D.USER.DOC or D.TSF.CONF are transparently encrypted and written to disk via mechanisms other than operating TSFI] Verify that the data written in Test 5 is not in plaintext form; and verify that the data can be decrypted by proper key and key material.

Test 5 and Test 6 should be performed for each mechanism not involving the operation of TSFIs described in the TSS.

Tracking

Issue #9