HCD0005 - CCMB review

Version: 1, Published: 2024-02-02

Impacted Documents

CPP_HCD_V1.0_supporting_doc

References

FTP_TRP.1/Admin Trusted path (for Administrators)

FCS_SSHC_EXT.1.2

A.3. Reporting

Issue Description

- In section 3.4.1.2, the second paragraph is not relevant to FTP_TRP.1/Admin Trusted path (for Administrators).
- In section 5.2.6.3.1, the last paragrah is metadata that should not be present.
- In section A.3, the first bullet point mentions that flaw identifiers returned from searches of public sources should be listed in public-facing reports. These raw search results are typically low quality information that may not be helpful to reproduce and thus should not be included in public-facing reports.

Resolution

- In section 3.4.1.2, delete the second paragraph.
- In section 5.2.6.3.1, delete the last paragrah.
- In section A.3, replace the statement in the first bullet point with a statement to list in the public-facing reports the terms and sources that were used for searching public sources following the instructions in section A.1.1, “Type 1 Hypotheses - Public-Vulnerability-based”.

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:

3.4.1.2. Guidance Documentation

The evaluator shall confirm that the operational guidance contains instructions for establishing the remote user sessions for each supported method.

~~The evaluator shall check to ensure that the operational guidance describes the type(s) of overwrite (e.g., single overwrite with zeros) of user document data that the TOE performs.~~

5.2.6.3.1. FCS_SSHC_EXT.1.2

Test objective: The purpose of these tests is to check the authentication of the client to the server using each claimed authentication method.

Test 1: For each claimed public-key authentication method, the evaluator shall configure the TOE to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH server to demonstrate the use of all claimed public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test.

Test 2: [Conditional] If password-based authentication method has been selected in the FCS_SSHC_EXT.1.2, then following the guidance documentation the evaluator shall configure the TOE to perform password-based authentication with a remote SSH server to demonstrate that the TOE can successfully authenticate using a password as an authentication method.

~~Now the HCD iTC has taken the text of the FCS_SSHC_EXT SFR from the ND SD v2.2 completely verbatim to form the FCS_SSHC_EXT SD text in the latest version of the HCD SD. Therefore, these AA changes should apply equally to the same SSHC AAs in the HCD SD as they do in the ND SD given that the AA text in both SDs are the same. As a result, the TSS, Guidance and Test changes for FCS_SSHC_EXT.1.2 and FCS_SSHC_EXT.1.5 should be made in Section 5.2.5 in the HCD SD.~~

A.3. Reporting

The evaluators shall produce two reports on the testing effort; one that is public-facing (that is, included in the non-proprietary evaluation report, which is a subset of the Evaluation Technical Report (ETR)), and the complete ETR that is delivered to the overseeing CB.

The public-facing report contains:

- ~~The flaw identifiers returned when the procedures for searching public sources were followed according to instructions in the Supporting Document per Section A.1.1, “Type 1 Hypotheses - Public-Vulnerability-based”;~~
- The terms and sources used when the procedures for searching public sources were followed according to instructions in the Supporting Document per Section A.1.1, “Type 1 Hypotheses - Public-Vulnerability-based”;

Tracking

Issue #16