Federal Office
for Information Security

Assurance Continuity Maintenance Report

BSI-DSZ-CC-1124-V3-2023-MA-01

CHERRY eHealth Terminal ST-1506, FW 4.0.23, HW 4.0.0

from

Cherry Digital Health GmbH

SOGIS
Recognition Agreement
for components up to
EAL 4

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [1] and the developer's Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-1124-V3-2023.

The change to the certified product is at the level of none-security-relevant functions in the source code including an update of the user guidance. The identification of the maintained product is indicated / by a new version number compared to the certified product. classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-1124-V3-2023 dated 6 June 2023 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-1124-V3-2023.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bonn, 5 January 2024

The Federal Office for Information Security

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 99 9582-0 - Fax +49 228 9582-5477 - Infoline +49 228 99 9582-111

Assessment

The IT product identified in this report was assessed according to the procedures on Assurance Continuity [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified product (Target of Evaluation, TOE) [3], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the CHERRY eHealth Terminal ST-1506, FW 4.0.23, HW 4.0.0, Cherry Digital Health GmbH, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements according to the procedures on Assurance Continuity [1]. In accordance with those requirements, the IAR describes (i) the changes made to the certified TOE, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The CHERRY eHealth Terminal ST-1506, FW 4.0.23, HW 4.0.0 was changed due to usability aspects (display layout and handling) as well as enhancing the compatibility with the connector. These changes do not modify any security-relevant functions in the source code and only have an effect on the user interface. The changes are therefore also related to an update of the user guidance [6] Configuration Management procedures required a change in the product identifier. Therefore the version number changed from FW 4.0.0, HW 4.0.0 to FW 4.0.23, HW 4.0.0

This change also covers an update of the Firmware Image 4.0.23 with the new SHA-256-Hashsum:

109c7d99f29cbf308f17d5c79550c171431f92c4cb8d59f510f394a4106a983e

Conclusion

The maintained change is at the level of none-security-relevant functions in the source code including an update of the user guidance. The change has no effect on product assurance, but the updated guidance documentation has to be followed.

Considering the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-1124-V3-2023 dated 6 June 2023 is of relevance and has to be considered when using the product.

Obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG[1] Section 9, Para. 4, Clause 2).

For details on results of the evaluation of cryptographic aspects refer to the Certification Report [3] chapter 9.2.

This report is an addendum to the Certification Report [3].

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

References

[1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.2, 30 September 2021

Common Criteria document “Assurance Continuity: SOG-IS Requirements”, version 1.0, November 2019

[2] IAR: Common-Criteria-Dokument Auswirkungsanalyse – FW-Update, Cherry Digital Health GmbH, V0.3, 21 September 2023 (confidential document)

[3] Certification Report BSI-DSZ-CC-1124-V3-2023 for CHERRY eHealth Terminal ST-1506, FW 4.0.0, HW 4.0.0, Bundesamt für Sicherheit in der Informationstechnik, 6 June 2023

[4] Security Target BSI-DSZ-CC-1124-V3-2023, Version 5.5, 2023-04-19, Security Target EAL3+ for eHealth Terminal ST-1506, Cherry Digital Health GmbH

[5] Configuration list for the TOE, ALC_CMS_HW, 1.1.1, 2023-01-31, ALC_CMS_SW, V2.1, 2023-11-23, BOM, V4.0.0, 2023-02-01, Bibliography V5.5, 2023-11-20 (confidential documents)

[6] eHealth Terminal ST-1506 – Handbuch für Administratoren (Teilenummer: 64410079), Version 08, 2023-11, Cherry Digital Health GmbH, SHA256-Hash: d450a53f7cef154af319482e9294372a12d65b6e63b96cd9cff0a7bd61384452