Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Jabra Engage 65 and Engage 75 with Embedded Software v4.2.0

Version 1.0, 04 August 2022

cyber.gov.au

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0 against Common Criteria EAL2+ALC_FLR.1.

The Target of Evaluation (TOE) is Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0. The TOE incorporates:

- Jabra Engage 65 or Jabra Engage 75 base station
- Jabra Convertible, Mono or Stereo headset.

The TOE enables secure two-way voice communications over a wireless link between the base station and the headset.

This report concludes that the TOE has complied with the Common Criteria (CC) evaluation assurance level EAL2 augmented with ALC_FLR.1 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP). The evaluation was performed by Teron Labs and was completed on 8 July 2022.

With regard to the secure operation of the TOE, the Australian Certification Authority (ACA) recommends that:

- users operate the TOE in the evaluated configuration and that organisational security policies concerning the TOE security environment are understood
- users review their operational environment and ensure security objectives for the operational environment can be met
- users understand TOE operation according to Jabra's Engage 65 and Engage 75 User manuals
- users specifically configure and operate the TOE according to Jabra's Common Criteria Supplementary Guidance
- users make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- users are aware that in the evaluated configuration the TOE base station and headset must only be paired by cradle placement
- users are aware that in the evaluated configuration the TOE is limited to one base station and one headset and is not used in conference call mode.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target [6] and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [6] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Jabra Engage 65 and Jabra Engage 75
Software version	Embedded Software v4.2.0
Security Target	*Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0 Security Target, Rev M, 28 July 2022*
Evaluation Technical Report	*Evaluation Technical Report 1.0 dated 31 July 2022* Document reference EFT-T025-ETR-1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Conformant and Part 3 Conformant, Version 3.1 Rev 5, April 2017
Methodology	Common Methodology for Information Technology Security, Version 3.1 Rev 5, April 2017
Conformance	EAL 2 augmented with ALC_FLR.1 (Basic flaw remediation)
Developer	GN Audio A/S Lautrupbjerg 7 2750 Ballerup

	Denmark
Evaluation facility	Teron Labs Pty Ltd Unit 3, 10 Geils Court Deakin ACT 2600 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0.

The TOE enables secure two-way voice communications over a wireless link between the base station and the headset.

The TOE uses the Digital Enhanced Cordless Telecommunications (DECT) wireless protocol and frequency band. The DECT signal and protocols used have been developed over many years and provide predictable and reliable performance on the reserved DECT frequency bands using a mixture of Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA) techniques.

In 2012 the DECT standards added the use of the Advanced Encryption Standard (AES) and longer keying parameters to improve security protocols for authentication and the protection of voice data. When used in the evaluated configuration the TOE base station and headset share keying material over a wired link (via the headset cradle) that protects the wireless link from person-in-the-middle and eavesdropping attacks. The TOE extends the DECT standards by increasing the length of keying parameters and utilising AES in 256 bit mode.

Being a wireless link in a fixed spectrum the TOE is intrinsically vulnerable to wireless availability attacks. However, as mentioned above, the DECT spectrum is well managed in most jurisdictions so accidental wireless interference issues are of less concern than for other wireless link technologies.

TOE Functionality

The TOE functionality that was evaluated is described in section 2.3.1 and section 2.4.2 of the Security Target [6].

TOE physical boundary

The TOE physical boundary is described in section 2.4.1 of the Security Target [6].

TOE Architecture

Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0 is a TOE that embodies a very simple two-part architecture that involves a base station communicating with a headset. In typical use the base station is connected to a computer or some other network audio source to perform the main TOE function of providing a wireless audio link.

To exercise other security functions provided by the TOE such as software update and boot failure audit a USB connected management computer is required to drive the TOE. The management computer runs a software application called Jabra Direct.

Clarification of scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [6].

Non-evaluated functionality and services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [4] for policy relating to using an evaluated product in an unevaluated configuration.

Security

The TOE Security Policy is a set of rules that defines how information within the TOE is managed and protected. The Security Target [6] contains a summary of the evaluated functionality and organisational security policies.

Usage

Evaluated configuration

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per operational guidance documentation [5].

Secure delivery

TOE delivery procedures

The software is pre-installed on the TOE hardware during the production of the TOE and the customer receives a functioning product. As a physical item the TOE is delivered by a tracked courier method, addressed to a specific person. Prior to deployment, seals and labels must be checked. A management computer must be connected to the TOE to read out the TOE internal product information to ensure it is correct.

The Common Criteria specific guidance is delivered to the users of the TOE through the Jabra secure web site. The process of delivery is as follows:

- an order is raised on the Jabra distribution channel
- an order of Jabra Engage 65 or Jabra Engage 75 units will raise a flag in the distributor’s system
- details for downloading the Common Criteria Guidance Supplement (i.e. the URL for the downloading of the document) are communicated to the end user or the other party who has placed the order
- the Common Criteria Guidance Supplement shall be downloaded from a Jabra secure download site. The web site will ask the user to check a tick box prior to download. By checking the tick box the user agrees to read the guidance supplement before deploying the TOE.

Installation of the TOE

The Common Criteria guidance documentation *Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0 Common Criteria Guidance Supplement* [5] contains all relevant information for the secure installation of the TOE.

Version verification

Both the base station and headset are specified at software version 4.2.0. This can be verified from a management computer running the Jabra Direct application while connected to the base station and headset.

Documentation and guidance

Generic guidance documentation is available on-line from Jabra for the Jabra Engage 65 and Jabra Engage 75 [5].

User Guides – https://www.jabra.com >> Support (Product Support) >> Search for your Jabra product

Common Criteria specific guidance documentation is available from Jabra on-line after an order is placed. This document is titled *Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0 Common Criteria Guidance Supplement, GNA SP 00022, Revision: B* [5].

Common Criteria material is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [4].

Secure usage

The evaluation of the TOE took into account certain organisational security policies to be followed in its operational environment. These policies must be followed in order to ensure the security objectives of the TOE are met:

- the TOE and management computer are physically protected
- each administrator for the TOE is competent for the role, they have received appropriate training and their actions are logged
- only Jabra Direct software is used for managing the TOE.

Other secure usage directives to be followed by TOE users include:

- the TOE base station and headset must only be paired by cradle placement
- the TOE is limited to one base station and one headset and must not be used in conference mode.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

Evaluation procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3* [1, 2].

Testing methodology was drawn from *Common Methodology for Information Technology Security, Version 3.1 Revision 5* [3].

The evaluation was carried out in accordance with the operational procedures of the Australian Information Security Evaluation Program [9].

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* were also upheld [8].

Functional testing

To gain confidence that the developer testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining the test coverage, test plans and procedures, and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

These developer tests are designed in such a way as to exercise the TOE security functional requirements and the TOE interfaces identified in the TOE design documentation.

Penetration testing

A vulnerability analysis of the TOE was conducted in order to identify any obvious vulnerability in the TOE and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

The evaluator performed a vulnerability analysis of the TOE in order to identify any obvious security vulnerability in the TOE, and if identified, to show that the security vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible security vulnerabilities in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

- time taken to identify and exploit (elapsed time)
- specialist technical expertise required (specialist expertise)
- knowledge of the TOE design and operation (knowledge of the TOE)
- window of opportunity
- IT hardware/software or other equipment required for exploitation.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

EAL2 provides assurance by a full security target and an analysis of the Security Functional Requirements (SFRs) in that security target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE Security Functionality (TSF), evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through the use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

Certification result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [6] and **has met** the requirements of Common Criteria EAL2+ALC_FLR.1.

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [7], the Australian Certification Authority **certifies** the evaluation of Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0 performed by the Australian Information Security Evaluation Facility, Teron Labs.

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual* [4].

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

The Australian Certification Authority also recommends:

- users operate the TOE in the evaluated configuration and that organisational security policies concerning the TOE security environment are understood
- users review their operational environment and ensure security objectives for the operational environment can be met
- users understand TOE operation according to Jabra's Engage 65 and Engage 75 User manuals

- users specifically configure and operate the TOE in accordance with Jabra’s Common Criteria Supplementary Guidance [5] available from Jabra
- users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- users are aware that in the evaluated configuration the TOE base station and headset must only be paired by cradle placement
- users are aware that in the evaluated configuration the TOE is limited to one base station and one headset and must not be used in conference call mode.

Annex A – References and abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 5, April 2017*

2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 5, April 2017*

3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 5, April 2017*

4. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism

5. Guidance documentation:

- *User Guides* – https://www.jabra.com >> Support (Product Support) >> Search for your Jabra product
- *CC Supplementary Guidance* – Jabra Engage 65 and Jabra Engage 75 with Embedded Software v 4.2.0 Common Criteria Guidance Supplement, GNA SP 00022, Revision: B

6. *Jabra Engage 65 and Jabra Engage 75 with Embedded Software v4.2.0 Security Target, Rev M, 28 July 2022*

7. Evaluation Technical Report - *EFT-T025 ETR 1.0 dated 31 July 2022*

8. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2-July-2014*

9. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf

Abbreviations

AES	Advanced Encryption Standard
AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
DECT	Digital Enhanced Cordless Telecommunications
EAL	Evaluation Assurance Level
FDMA	Frequency Division Multiple Access
HTTPS	Hypertext Transfer Protocol Secure
SHA256	Secure Hash Algorithm 256 bit digest
TDMA	Time Division Multiple Access
TLS 1.2	Transport Layer Security version 1.2
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface
USB	Universal Serial Bus