Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Ziperase Drive Erasure Software v3.0.2

Version 1.0, 06 September 2024

Document reference: AISEP-CC-CR-2024-EFT-T042-CR-V1.0
(Certification expires five years from certification report date)

cyber.gov.au

ACSC Australian Cyber Security Centre

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of Ziperase Drive Erasure Software v3.0.2 against Common Criteria EAL2.

The Target of Evaluation (TOE) is Ziperase Drive Erasure Software v3.0.2. The TOE incorporates:

- Ziperase array-3.0.2.iso for the TOE in an appliance configuration
- Ziperase command-center-3.0.2.iso for the TOE in a network configuration
- Ziperase core-3.0.2-x86_64.iso for the TOE as standalone configuration.

The TOE is used as one of the selected configurations for booting up a target host that securely erases the attached drive.

This report concludes that the TOE has complied with the Common Criteria (CC) evaluation assurance level EAL2 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 17 May 2024

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

- ensure that the TOE operated in the evaluated configuration and that any assumptions 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 Ziperase User manuals
- users specifically configure and operate the TOE according to Ziperase's Common Criteria Supplementary Guidance and pay attention to all security warnings
- users need to understand the strengths and limits of each algorithm as described in the Common Criteria Guidance Supplement and related documentation
- users need to be aware that secure erasing methods for SSD drives are different from ones for traditional magnetic drives.

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 Ziperase Drive Erasure Software v3.0.2.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Ziperase Drive Erasure Software v3.0.2
Software version	v3.0.2
Security Target	*Ziperase Drive Erasure Software v3.0.2 - Security Target Version 1.0, 17 July 2024*
Evaluation Technical Report	*Evaluation Technical Report 1.0 dated 17 July 2024* Document reference EFT-T042-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
Developer	Ziperase 6500 River Pl Blvd Austin, TX 78730

	United States of America
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 Ziperase Drive Erasure Software v3.0.2.

The TOE is a secure drive erasure tool developed by Ziperase Ltd. It may be used in a standalone configuration, network configuration or appliance configuration. In each configuration, the TOE is used for booting up a target host which contains or is attached to a drive that needs to be erased in a secure manner.

Once the target host boots up with the TOE, the TOE software implements a minimalistic Graphical User Interface (GUI) which allows the operator to select the drive to be erased, the erasure algorithm as well as set other parameters for the erasure. Once the operator proceeds with the erasure, the TOE erases the drive of the target host in accordance with the selected algorithm and reports the findings to the operator.

The Ziperase Drive Erasure Software v3.0.2 implements a rich set of erasure standards suitable for different drive types. The exact same erasure algorithms are also available when the TOE is operated in each configuration. Many are legacy standards which may only be required for specific, rare use cases.

The TOE generates an erasure report and verifies that the erasure has been completely carried out in accordance with the erasure standard.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.2 of the Security Target [6].

TOE physical boundary

The TOE physical boundary is described in section 1.2.3 of the Security Target [6].

TOE Architecture

Ziperase Drive Erasure Software v3.0.2 is an ISO file distributable as one of three configurations. The TOE interacts with the drive API and other components of the operational environment.

The TOE is a standalone executable software booted locally or remotely from a bootable media. All security enforcement functions of the TOE are implemented by the state machine enforced by the erasure application.

The TOE included a minimalistic operating system which provides the basic functions for the erasure application. The operating system is supported by Grub software, which implements the boot sequence of Linux and a modified intrd daemon that implements the boot up from bootable media.

The TOE is distributed with a SHA-512 checksum of the .iso image. The user is to verify the checksum. Only if the checksum is correctly verified, may the user proceed with the transition of the TOE from the .iso representation to an executable representation.

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 distributed as a package-based ISO image. Ziperase provides the user with a link to an .iso file, a SHA-512 checksum of the file, security guidance documentation and instructions on how to verify the authenticity of the .iso file. The user follows the link, downloads the software image and user guidance and verifies the authenticity using the SHA-512 checksum. The TOE may download to, and verify on the Host computer or dedicated storage environment.

The Common Criteria specific guidance is delivered to the users of the TOE through download of the security guidance documentation. The process of delivery is as follows:

- the TOE software is downloaded via a link given by an authorised Ziperase Sales Representative
- TOE guidance documentation is also downloaded from the same website. If the link does not function correctly, the user is to contact the sales representative for a resolution
- a TOE checksum is made available. The user must download the software with the checksum to a device with a message digest computation software installed. Any software trusted by the user of the TOE is acceptable
- further delivery instructions on the TOE are listed in the Common Criteria Supplement Guidance document [5].

Installation of the TOE

The Common Criteria guidance documentation *Ziperase Drive Erasure Software v3.0.2 Common Criteria Guidance Supplement* [5] contains all relevant information for the secure installation of the TOE.

Version verification

The software version is specified as 3.0.2. This can be verified from a management computer running the SHA-512 checksum digest through a message digest computation software. Where the checksum and the software match, the version is authentic and may be used. Otherwise, please contact Ziperase account representative for further instructions.

Documentation and guidance

All user guides and Common Criteria specific guidance documentation is available from Ziperase after an order is placed.

Common Criteria specific guidance documentation is titled *Ziperase Drive Erasure Software v3.0.2 Common Criteria Guidance Supplement v1.0, 16 May 2024*

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 and logically protected
- each administrator for the TOE is competent for the role, they have received appropriate training and their training records are stored appropriately with applicable HR policies and procedures
- the TOE verifies the licenses possessed by the user. By default, the user possesses zero licenses, with all licenses obtained by the user from Ziperase prior to the operation of the TOE.

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

- fulfilling legal or regulatory secure data erasure obligations
- fhe TOE in a network configuration is operated on a secure, trusted network where violation of the security of the TOE is not allowed.

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.

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 Ziperase Drive Erasure Software v3.0.2 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:

- ensure that the TOE operated in the evaluated configuration and that any assumptions 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 Ziperase Drive Erasure User manuals

- users specifically configure and operate the TOE in accordance with Ziperase's Common Criteria Supplementary Guidance [5] available from Ziperase and pay attention to all security warnings
- users need to understand the strengths and limits of each algorithm as described in the Common Criteria Guidance Supplement and related documentation
- users need to be aware that secure erasing methods for SSD drives are different from ones for traditional magnetic drives.

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. *Ziperase Drive Erasure Software v3.0.2 Common Criteria Guidance Supplement Version 1.0, 16 May 2024*
6. *Ziperase Drive Erasure Software v3.0.2 - Security Target Version 1.0, 17 July 2024*
7. Evaluation Technical Report - *EFT-T042 ETR 1.0 dated 17 July 2024*
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/resources-business-and-government/assessment-and-evaluation-programs/australian-information-security-evaluation-program

Abbreviations

AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
ISO	Optical Disk Image
IT	Information Technology
SHA512	Secure Hash Algorithm 512 bit digest
SSD	Solid State Drive
TOE	Target of Evaluation
TSF	TOE Security Function
USB	Universal Serial Bus