Certification Report

MindSpore 1.2

Sponsor and developer: ***Huawei Technologies Co., Ltd.***
D4 Area Administration Building, Southern Factory of Huawei Technologies Co., Ltd
No 6 Xincheng Avenue, Songshan Lake Technology Industrial Park
Dongguan City, 523808,
People's Republic of China.

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0415138-CR**

Report version: **1**

Project number: **0415138**

Author(s): **Andy Brown, Wouter Slegers and Wim Ton**

Date: **04 April 2022**

Number of pages: **12**

Number of appendices: **0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

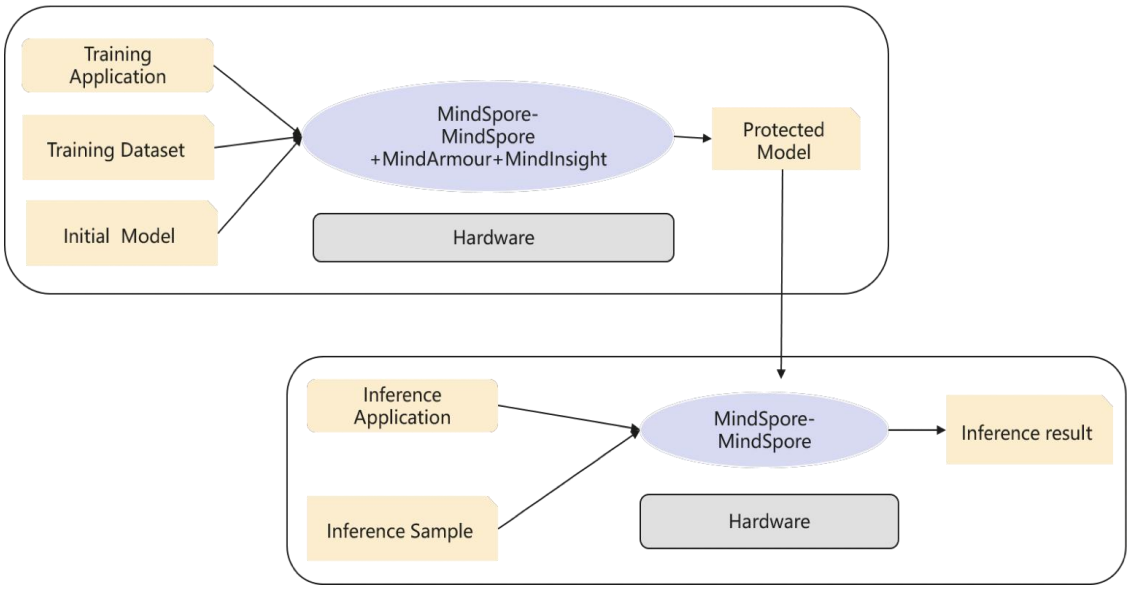
1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the MindSpore 1.2. The developer of the MindSpore 1.2 is Huawei Technologies Co., Ltd. located in Dongguan City, People's Republic of China and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

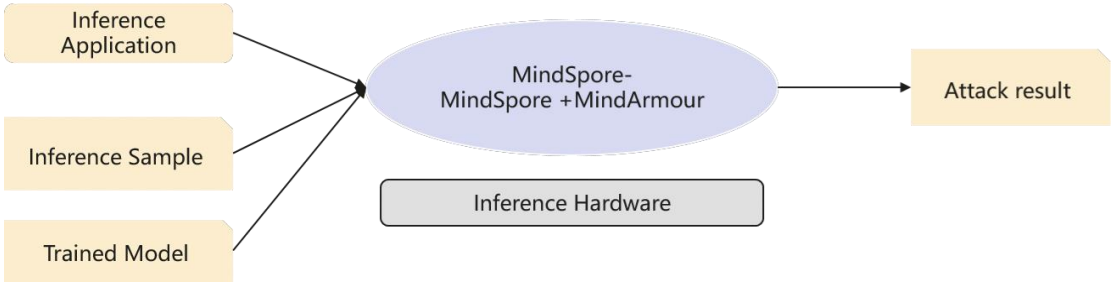
The TOE is an open source deep learning training/inference framework software developed by Huawei. It will be referred to as the TOE throughout this document.

MindSpore is provided as a library that is used by AI Application developers to provide AI services.

In the evaluated configuration, an AI Application developer will use MindSpore-MindSpore along with the MindSpore-MindArmour library to improve the generated AI Application deep learning models into a protected model or to attack the original model in the field of Computer Vision. The security functionality allows for evaluation and comparison of the robustness of models, leading to model design improvements; it is therefore an important part of the security functionality.



Model hardening use case included in [ST] scope



Attack use case included in [ST] scope

Out of scope is the creation of AI Applications that define and train a deep learning model using a training dataset and MindSpore. Also out of scope is the creation of AI Applications that use trained models and MindSpore to conduct inference of samples.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 04 April 2022 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the MindSpore 1.2, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the MindSpore 1.2 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL2: augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the MindSpore 1.2 from Huawei Technologies Co., Ltd. located in Dongguan City, People's Republic of China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	MindSpore	1.2.0
	MindArmour	1.2.1
	MindInsight	1.2.0

To ensure secure usage a set of guidance documents is provided, together with the MindSpore 1.2. For details, 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE provides the following security functionalities:

- Generation of adversarial samples
- Hardening of inference model against adversarial samples.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

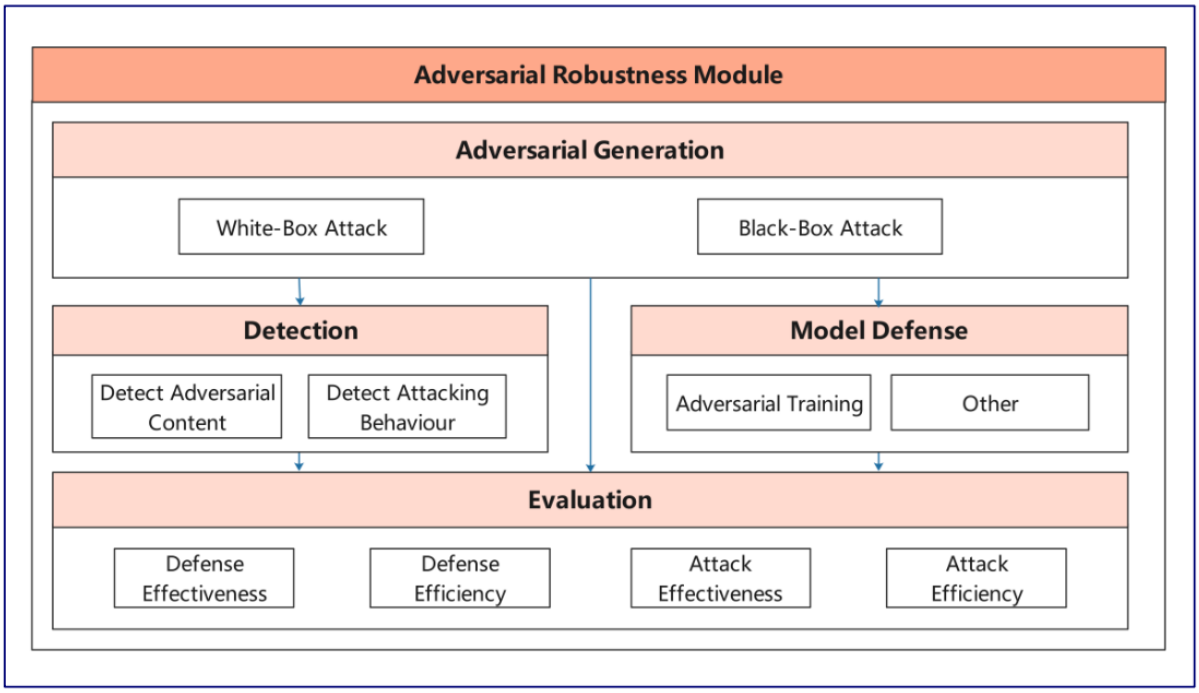
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:



Logical architecture of the TOE.

The TOE is purely a software TOE. The whole framework is labelled as MindSpore 1.2, comprised of the following components:

- MindSpore 1.2.0
- MindArmour 1.2.1
- MindInsight 1.2.0

The software components are used together to generate, attack, defend and apply inference to computer vision deep learning models.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
MindSpore Interfaces Specification Release r1.2.pdf	1.2
MindArmour Interfaces Specification Release r1.2.pdf	1.2
MindInsight Interfaces Specification Release r1.2.pdf	1.2
CC MindSpore 1.2-AGD_PRE _V0.8.pdf	0.8
CC MindSpore 1.2-AGD_OPE _V0.8.pdf	0.8

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer created test cases intended to fully test the TSF related to each SFR, plus test cases intended to test the TSFI APIs.

In order to perform the testing described above, the developer prepared a complete set of scripts to run each test case plus the necessary scripts to satisfy the pre-conditions and/or ordering dependencies.

The evaluator repeated all the developer test cases.

The evaluator created an additional test case test intended to verify the version of the TOE, and additional test cases intended to further test the accuracy of the adversarial samples created by the TOE on other AI models.

2.6.2 Independent penetration testing

The penetration test was focused on testing the TOE protected models against adversarial samples created by other AI frameworks.

The total test effort expended by the evaluators was 6 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The evaluator tested the TOE in the following configuration: MindSpore v1.2.

This is one of the configurations stated in the *[ST],* and representative of all configurations. Mindspore components are not dependent on platform architecture. The different architecture packages stated in the *[ST]* are the result of the installers adapted to different platform architecture. The function of the TOE is not impacted in the adaptation.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number MindSpore 1.2.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the MindSpore 1.2, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 2 augmented with ALC_FLR.2** .

This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must 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. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

3 Security Target

The MindSpore 1.2 Security Target, version 1.3.6, 01 April 2022 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AI	Artificial Intelligence
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report MindSpore v1.2 – EAL2+, 21-RPT-767, Version 6.0, 01 April 2022
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	MindSpore 1.2 Security Target, version 1.3.6, 01 April 2022

(This is the end of this report.)