Certification Report

Cisco Unified Computing System Standalone, Version 4.0(4i)

Sponsor and developer:	***Cisco Systems Inc*** **170 West Tasman Dr.** **San Jose, CA 95134** **USA**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0038305-CR**
Report version:	**1**
Project number:	**0038305**
Author(s):	**Andy Brown**
Date:	**24 April 2020**
Number of pages:	**11**
Number of appendices:	**0**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Headoffice:
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 Dutch Chamber of Commerce 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 license 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, in order 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.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 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. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Cisco Unified Computing System Standalone, Version 4.0(4i). The developer of the Cisco Unified Computing System Standalone, Version 4.0(4i) is Cisco Systems Inc located in San Jose, USA 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 a network device that consists of hardware and software components that support Cisco Unified Systems, running in standalone mode. The TOE features a role based access control policy to control the separation of administrative duties and provide a security log of all changes made.

In standalone mode each UCS C-Series and S Series server runs as an independent system. The Cisco Integrated Management Controller (CIMC) manages each platform as an individual entity in a Data Centre or across remote locations.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 21 April 2020 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 Cisco Unified Computing System Standalone, Version 4.0(4i), 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 Cisco Unified Computing System Standalone, Version 4.0(4i) 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 provides sufficient evidence that the TOE meets the EAL2.

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]*.

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. It should be noted that the certification results only apply 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 releasable for public review.

2 Certification Results

2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the Cisco Unified Computing System Standalone, Version 4.0(4i) from Cisco Systems Inc located in San Jose, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Cisco UCS C-Series Rack Servers (C220 M5, C240 M5, C480 M5 and C480 ML M5)	N/A
	Cisco UCS S-Series Rack Servers (S3260 M5)	N/A
	Virtual Interface Cards (security non-enforcing and listed in [ST] section 1.3.3)	N/A
Software	Cisco Integrated Management Controller (CIMC)	4.0(4i)

To ensure secure usage a set of guidance documents is provided together with the Cisco Unified Computing System Standalone, Version 4.0(4i). Details can be found in section 2.5 of this report.

2.2 *Security Policy*

The major security features provided by the TOE are summarized as follows:

The TOE provides audit information to assist the administrator in monitoring the security state of the TOE as well as trouble shooting various problems that arise throughout the operation of the system.

The TOE provides local administrator authentication using username and password, or authenticate administration via a remote authentication server. However only one of them can be select at a time, not both.

The TOE can be managed using the graphical user interface (over TLS 1.2), the command line (over SSHv2 or by local console access via the RS-232 port), or by manipulating an XML API. The interfaces all operate on the same XML data structures and provide identical functionality. In addition the UCS provides SNMPv3 to export system traps and support remote monitoring (read only). This interface supports SHA authentication and AES-128 encryption for protecting the confidential system information.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. The TOE provides the Authorized Administrators the capability to change the timezone in order to update the TOE’s clock to maintain a reliable timestamp. The timestamp is updated accordingly when the timezone is changed.

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles. A role defines the privileges of a user in the system that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in 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.

Note: A syslog server is required for receiving and reviewing audit messages of failed administrative actions. Successful actions are logged to the local audit logs as well as to the remote syslog server. Failed authentication attempts are not logged to the local audit log but are sent to a remote syslog server.

2.4 Architectural Information

The general architecture consists of two subsystems:

- The Processing Node subsystem in which only CMIC chip is the only SFR enforcing part which provides the following security functions:
    - I&A
    - Management functions
    - Logging
    - Secure communication
    - Management interfaces:CLI and GUI

- The UCS CIMC Client Subsystem which is a java-based application running in a non-TOE browser on a non-TOE workstation:
    - It is used to connect to the UCS CIMC chip running on the server and perform management operations.
    - It makes no decision as the CIMC chip decides whether actions are allowed.

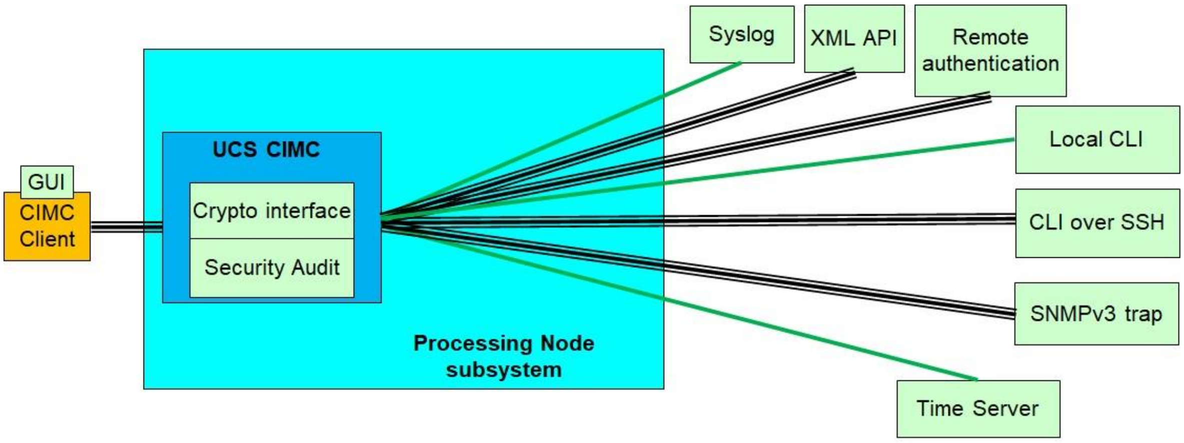

Figure 1: TOE Architecture

2.5 Documentation

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

Identifier	Version
Cisco Unified Computing System Standalone version 4.0(4i) Common Criteria Operational User Guidance and Preparative Procedures	1.0

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 tests consisted of 23 tests. These tests covered most of the TSFI and SFRs and include both positive and negative tests. The developer and evaluator tested using different device models to maximize the coverage over multiple devices. The evaluator repeated 5 tests putting emphasis on those tests covering verification of the SSH remote access protocol, verifying user account privileges, certain claims in the Security Target (e.g. role-based access control) and protection of audit logs and their time stamp.

In addition to the developer tests, the evaluator derived and executed 10 additional functional tests.

2.6.2 Independent Penetration Testing

The evaluators performed 10 penetration tests. These were derived from a vulnerability analysis comprised of 3 parts:

1. SFR mapping table

   The evaluator applied their knowledge of attacks applicable to the TOE based on the information gathered from all evaluation evidence.

2. Public domain analysis

   The evaluator performed a public domain vulnerability search for TOE specific items (TOE name, TOE-type, secure libraries, etc.)

   The evaluator used the websites provided by NSCIB as a basis to perform the search.

3. Network scanning tools

   The evaluator ran vulnerability scanning tools and analysed the results to identify potential vulnerabilities.

2.6.3 Test Configuration

The following parts made up the TOE under test, and were configured as show in Figure 2:

Identifier	Product name	Firmware
UCSC-C220-M5	Cisco UCS C220 M5 Rack Server	4.0(4i)

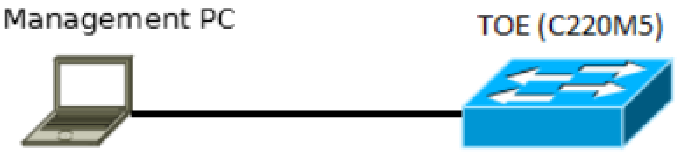

Figure 2: Baseline test setup

2.6.4 Testing 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.

2.7 Re-used evaluation results

There is no re-use of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Cisco Unified Computing System Standalone, Version 4.0(4i). Details of the hardware models included in the TOE are provided in section 2.1

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the [ETR] which references a 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 Cisco Unified Computing System Standalone, Version 4.0(4i), to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL2**. 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 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details with respect to the resistance against certain attacks.

Note: To record failed authentication attempts, the user needs to configure a remote syslog server. Successful actions are logged to the local audit logs as well as to the remote syslog server. Failed authentication attempts are not logged to the local audit log but are sent to a remote syslog server.

In addition 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.

3 Security Target

The Cisco Unified Computing System Standalone, Security Target, Version 1.0, 14 April 2020 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

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
SHA	Secure Hash Algorithm
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 Cisco Unified Computing System Standalone, Version 4.0(4i), 20-RPT-046, Version 2.0, 15 April 2020.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[ST] Cisco Unified Computing System Standalone, Security Target, Version 1.0, 14 April 2020.

(This is the end of this report).