TÜVRheinland®
Precisely Right.

Certification Report

Cisco UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C- Series Rack-Mount Servers, S-Series Storage Servers, 2200/2300 Series Fabric Extenders, and 6200/6300/6400 Series, Fabric Interconnects with UCSM 4.0(4b)

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-228723-CR**
Report version:	**1**
Project number:	**228723**
Author(s):	**NLNCSA/name of external certifier**
Date:	**17 October 2019**
Number of pages:	**14**
Number of appendices:	**0**

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

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-19-228723**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Cisco Systems Inc** **170 West Tasman Dr. San Jose, CA 95134 USA**
Product and assurance level	**Cisco UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C- Series Rack-Mount Servers, S-Series Storage Servers, 2200/2300 Series Fabric Extenders, and 6200/6300/6400 Series, Fabric Interconnects with UCSM 4.0(4b)** Assurance Package: ▪ EAL2
Project number	**228723**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity

Date of issue : **08-11-2019**

Certificate expiry : **08-11-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

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.

TÜVRheinland®
Precisely Right.

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 UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C- Series Rack-Mount Servers, S-Series Storage Servers, 2200/2300 Series Fabric Extenders, and 6200/6300/6400 Series, Fabric Interconnects with UCSM 4.0(4b) which is shortened to “UCS System” in the remainder of this section. The developer of the UCS System 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 unified computing solution, which provides access layer networking and servers. The TOE consists of hardware and software components that support Cisco's unified fabric, which run multiple types of data-centre traffic over a single converged network adapter. The UCS features a role based access control policy to control the separation of administrative duties and provide a security log of all changes made.

A single Cisco Unified Computing System scales to up to forty chassis and three hundred twenty blade servers or rack-mount servers, all of which are administered through a single management entity called the Cisco UCS Manager.

The Fabric Interconnects and Fabric Extenders are based on the same switching technology as the Cisco Nexus 5000 Series. Fabric Interconnects also provide additional centralized management capabilities that form the basis of the Cisco UCS Manager.

Cisco UCS implements Cisco unified fabric within racks and groups of racks, supporting Ethernet and Fibre Channel protocols over 10 Gigabit Cisco® Data Center Ethernet and Fibre Channel over Ethernet (FCoE) links. The result of this network unification is a reduction by up to two-thirds of the switches, cables, adapters, and management points. All devices in a system remain under a single management domain, which remains highly available through the use of redundant components.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 08 October 2019 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 UCS System, 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 UCS System 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 assurance requirements for the evaluated security functionality.

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 UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C- Series Rack-Mount Servers, S-Series Storage Servers, 2200/2300 Series Fabric Extenders, and 6200/6300/6400 Series, Fabric Interconnects with UCSM 4.0(4b) from Cisco Systems Inc located in San Jose, USA. Hereinafter the TOE name is shortened to "UCS System".

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Cisco UCS 5108 Blade Server Chassis	N/A
	Cisco UCS Blade Servers:B200 M5, and B480 M5	N/A
	Cisco UCS C-Series Rack Servers: C125 M5, C220 M5, C240 M5, C480 M5 and C480 ML M5	N/A
	Cisco UCS C4200 Rack Server Chassis	N/A
	Cisco UCS S-Series Rack Servers: S3260 M5	N/A
	Network Adapters and Virtual Interface Cards compatible with B-Series Servers: Cisco UCS VIC 1340, Cisco UCS VIC 1440, Cisco UCS VIC 1480	N/A
	Network Adapters and Virtual Interface Cards compatible with C-Series Servers: Cisco UCS VIC 1225, Cisco UCS VIC 1225T, Cisco UCS VIC 1385, Cisco UCS VIC 1387, Cisco UCS VIC 1455, Cisco UCS VIC 1457	N/A
	Network Adapters and Virtual Interface Cards compatible with S-Series Servers: Cisco UCS VIC 1227, Cisco UCS VIC 1455, Cisco UCS VIC 1387	N/A
	Cisco UCS Fabric Interconnects: 6324, 6332, 6332-16UP, and 6454	N/A
	Cisco UCS Fabric Extenders: 2204XP, 2208XP, 2304	N/A
	Nexus Fabric Extender: 2232PP, 2232TM-E and 2348UPQ	N/A
Software	Cisco Unified Computing System (UCS) version 4.0(4b)	4.0(4b)

To ensure secure usage a set of guidance documents is provided together with the UCS System. Details can be found in section "Documentation" 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 UCS 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 separates the networks by using VLANs and VSANs. VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical local-area network (LAN) infrastructure into different subnets so that VLAN packets are presented to interfaces within the same VLAN.

Virtual SAN (VSAN) technology partitions a single physical Storage Area Network (SAN) into multiple VSANs. Traffic is contained within VSAN boundaries and devices reside only in one VSAN thus ensuring absolute separation between user groups. This ensures the confidentiality of data traversing the VSAN from users and devices belonging to other VSANs.

The TOE utilizes role based access control to restrict or authorise system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) 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 and locales.

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. The following note is in scope for the certified TOE:

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 four subsystems:

- The *Fabric Interconnect (FI)* subsystem providing:
  - Unifying up to 320 servers within a single system domain
  - Connecting every server resource in a system
  - An execution platform for the UCS Manager server software that provides:
    - General OS functionalities.
    - Security audit
    - Cryptography
    - Data protection by using role-based access control and information flow control

        - Identification and authentication
        - User management
        - Protection of the TSF

- The *Fabric Extender (FEX) subsystem* providing:
    - Traffic aggregation/de-aggregation between FI and servers
- The *Processing Node subsystem in which* only CMIC chip and vNIC are part of the TOE:
    - CIMC monitors physical state of the servers' hardware.
    - CIMC supports OS independent/pre-OS management.
    - vNIC (Virtual network interface card) sends/receives information to the FI and user traffic to FI.
- The UCS Manager Client Subsystem which is a java-based application running in a nonTOE browser on a non-TOE workstation:
    - It is used to connect to the UCS Manager server running on the FI and perform management operations.
    - It makes no decision as the FI subsystem decides whether actions are allowed.

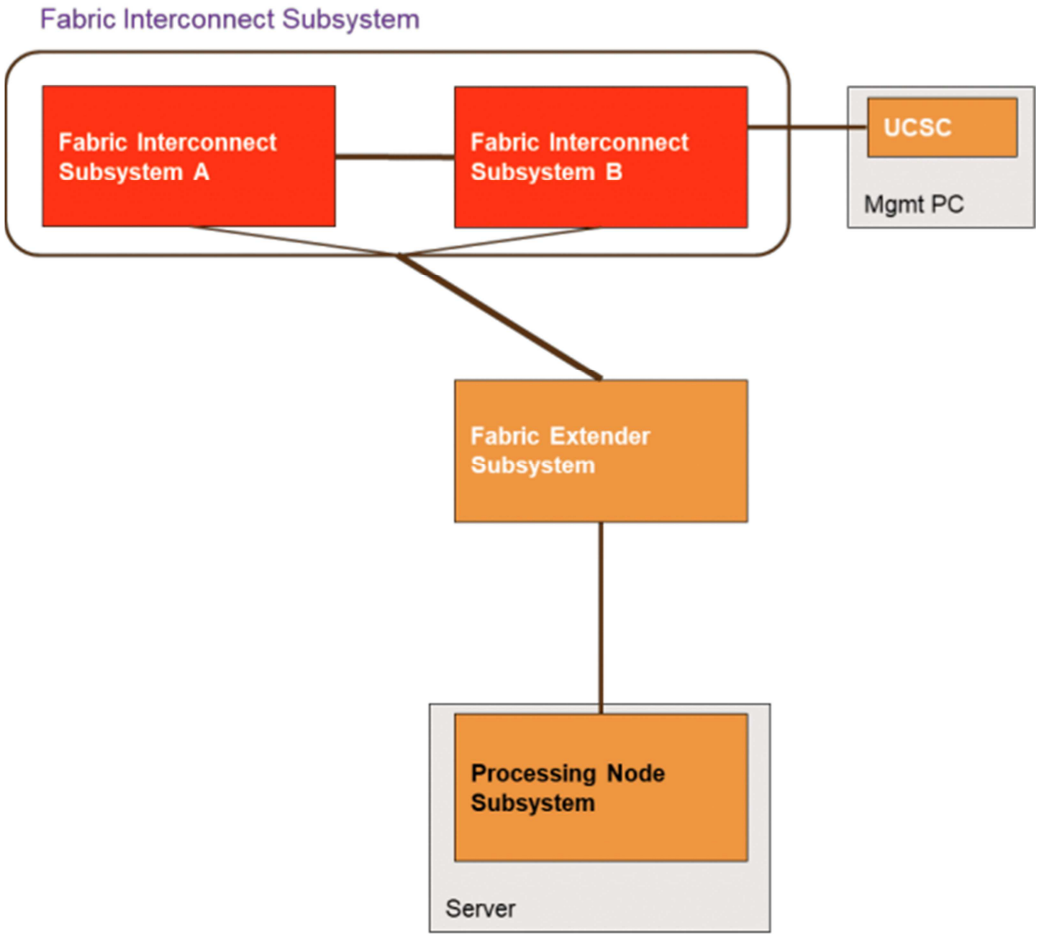

Figure 1 TOE Architecture

2.5 Documentation

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

Identifier	Version
Cisco Unified Computing System (UCS) version 4.0(4b) Common Criteria Operational User Guidance and Preparative Procedures	V1.0

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 consist of 42 tests, some of which were quite extensive. These tests cover all TSFI and all SFRs and include both positive and negative tests. Brightsight repeated 9 of the 42 developer tests.

In addition to the developer tests, the evaluator derived and executed 8 additional functional tests.

2.6.2 Independent Penetration Testing

The evaluators performed 17 penetration tests. These were derived from a vulnerability analysis comprised of 3 parts:

1. SFR mapping table

   The evaluator applies his/her knowledge of attacks applicable to the TOE based on the information gathered from all evaluation evidence.

2. Public domain analysis

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

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

3. Network scanning tools

   The evaluator runs 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
UCS-FI-6454	Cisco UCS 6454 Fabric Interconnect	4.0(4b)
UCSC-C220-M5	Cisco UCS C220 M5 Rack Server	4.0(4b)

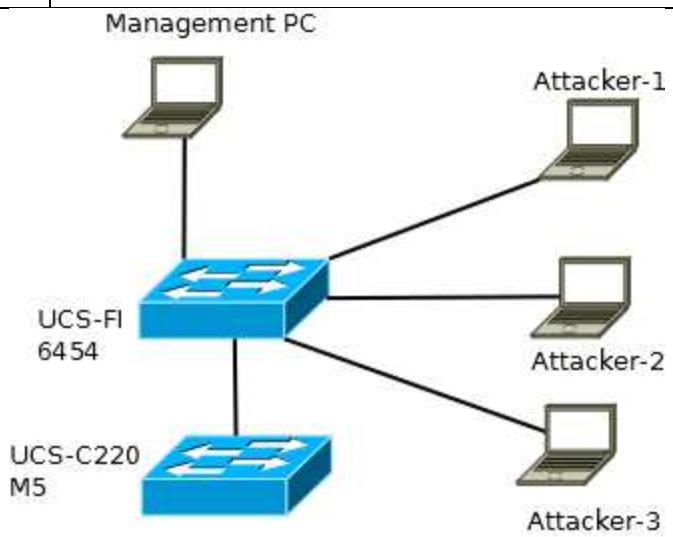

Figure 2: Baseline test setup.

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 Evaluated Configuration

The TOE is defined uniquely by its name and version number Cisco UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C- Series Rack-Mount Servers, S-Series Storage Servers, 2200/2300 Series Fabric Extenders, and 6200/6300/6400 Series, Fabric Interconnects with UCSM 4.0(4b). Details of the hardware models included in the TOE are provided in section 2.1.

2.8 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 UCS System, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.9 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 (UCS), Version 1.0, 18 September 2019 *[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
TOE	Target of Evaluation
SAN	Storage Area Network
SHA	Secure Hash Algorithm
VLAN	Virtual LAN
VSAN	Virtual SAN (VSAN)

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 UCS 5100 Series Blade Server Chassis, B-Series Blade Servers, C- Series Rack-Mount Servers, S-Series Storage Servers, 2200/2300 Series Fabric Extenders, and 6200/6300/6400 Series, Fabric Interconnects with UCSM 4.0(4b), 19-RPT-735, 2.0, 08 October 2019.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September April 2017.
[ST]	Cisco Unified Computing System (UCS), Version 1.0, 18 September 2019.

(This is the end of this report).