Certification Report

Cisco HyperFlex 4.5(2a) Systems HX Series

Sponsor and developer: ***Cisco Systems, Inc.***
170 West Tasman Drive
San Jose, CA 95134
USA

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

Report number: **NSCIB-CC-215885-CR2**

Report version: **1**

Project number: **215885_2**

Author(s): **Denise Cater**

Date: **13 January 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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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 Cisco HyperFlex 4.5(2a) Systems HX Series. The developer of the Cisco HyperFlex 4.5(2a) Systems HX Series 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 manages the storage of a storage cluster that has a minimum three servers (HyperFlex HX Series Nodes (Converged Host)) with Solid-state disk (SSD) and Hard-disk drives (HDD) attached storage. The clustered servers are networked with switches and fabric interconnects. Optionally, non-storage servers, (compute nodes), can be included in the storage cluster. HX Data Platform manages the storage for the data and VMs stored on the associated storage cluster.

The HyperFlex HX Series installer is loaded on a UCS platform that is networked to the storage cluster to be managed. The initial cluster includes at least three HyperFlex HX Series Nodes. The HyperFlex HX Series includes HyperFlex Connect (HX Connect) GUI, which is used as the primary management tool for Cisco HyperFlex. Through this centralized point of control for the cluster, administrators can create volumes, monitor the data plat-form health, and manage resource use.

The TOE was evaluated initially by SGS Brightsight B.V. located in Delft, The Netherlands and was certified on 25 November 2019. The re-evaluation of the TOE has also been conducted by SGS Brightsight B.V. and was completed on 12 January 2022 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are the addition of a new hardware model and update of the software from version 3.5(2a) to 4.5(2a).

The security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made, as well as renewed testing.

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 HyperFlex 4.5(2a) Systems HX Series, 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 HyperFlex 4.5(2a) Systems HX Series 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 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]* (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 Cisco HyperFlex 4.5(2a) Systems HX Series 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 HyperFlex HXAF220c – M5SX All – Flash Node	HXAF 220c – M5SX
	Cisco HyperFlex HXAF240c – M5SX All – Flash Node	HXAF 240c – M5SX
	Cisco HyperFlex HX220c – M5SX Hybrid Node	HXAF 240c – M4SX
	Cisco HyperFlex HX240c – M5SX Hybrid Node	HXAF 220c – M4S
	Cisco HyperFlex HXAF220c - M5SN NVMe Node	HXAF220c - M5SN NVMe
	Cisco HyperFlex HX240c – M5L Hybrid Node	HX220c – M5SX
	Cisco HyperFlex HXAF220c – M4S All-Flash Node	HX240c – M5SX
	Cisco HyperFlex HXAF240c – M4SX All-Flash Node	HX240c – M5L
	Cisco HyperFlex HX220c – M4S Hybrid Node	HX220c – M4S
	Cisco HyperFlex HX240c – M4SX Hybrid Node	HX240c – M4SX
Software	Cisco HyperFlex HX Data Platform Software for VMware ESXi	4.5(2a)

To ensure secure usage a set of guidance documents is provided, together with the Cisco HyperFlex 4.5(2a) Systems HX Series. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Security audit:
  - The TOE generates audit messages that identify specific TOE operations.
- User data protection
  - The TOE provides the Authorized Administrator with the ability to control remote host (VMs) access to the TOE Converged hosts, clusters and datastores with whitelisting.
- Identification and authentication
  - The TOE provides authentication services for the Authorized Administrator to connect to the TOE’s HX Connect GUI and HXCLI administrator interfaces
- Secure Management
  - The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE.
- Protection of the TSF
  - The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication and limit configuration options to the Authorized Administrator.

- Resource Utilization
  - The TOE protects against unavailability of capabilities and system resources caused by failure or degradation of services by supporting redundancy and failover capabilities of the storage management network and the storage data networks.
- TOE Access
  - The TOE enforces the termination of inactive sessions after an Authorized Administrator configurable time-period has expired.
- Trusted Path
  - The TOE allows trusted paths to be established to itself from remote administrators over HTTPS/TLSv1.2 for remote HX Connect GUI and SSHv2 for remote HXCLI access.

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 TOE is installed in a hypervisor environment, such as VMware vSphere where it manages the storage clusters and data stores that has a minimum three servers, (TOE Converged hosts), with SSD and HDD attached storage. The clustered servers (TOE Converged hosts) are networked with switches and fabric interconnects. Optionally, non-storage servers, (compute nodes), can be included in the storage cluster (TOE Converged hosts). HyperFlex HX Series manages the storage for the data and VMs stored on the associated storage cluster (TOE Converged hosts).

The logical architecture of the TOE can be depicted as follows:

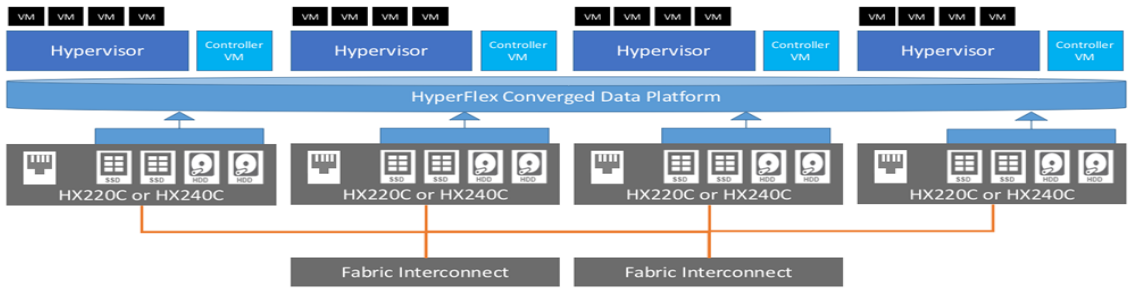

Figure 1. Logical architecture of the TOE.

2.5 Documentation

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

Ref	Identifier	Version
[AGD]	Cisco HyperFlex Systems HX Series Common Criteria Operational User Guidance and Preparative Procedures	Version: 3.0 15 December 2021

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 has testing of all TSFI identified in the functional specification. For both the original evaluation and this re-evaluation, the evaluator's strategy to identify which test cases to repeat took into account the verification of the SSH and HTTPS protocols (which are remotely accessible) and their configuration which can be prone to errors. In addition the evaluators devised independent test cases focusing on the verification of other core security functions provided by the TOE and the verification that the user guidance provides all the necessary steps for secure configuration of the TOE.

The developer made a test environment available for use by the evaluators.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR design analysis: Based on the information obtained in the evaluation evidence, the SFR implementation details were examined. The aspects described in CEM annex B were considered. During this examination several potential vulnerabilities were identified.
- Additional security analysis: When the implementation of the SFR was understood, a coverage check was performed on the relevant aspects of all SFRs. This expanded the list of potential vulnerabilities.
- Public vulnerability search: The evaluator performed public domain vulnerability search based on the TOE name, TOE type, and identified 3rd party security relevant libraries and/or services. Several additional potential vulnerabilities were identified during a search in the public domain.
- The potential vulnerabilities identified were analysed, and some of the potential vulnerabilities were concluded not exploit within in the Basic attack potential, or covered by guidance. For remaining potential vulnerabilities, penetration tests were devised.

For both the original evaluation and this re-evaluation, the evaluator focused on the following in the generation of their penetration tests:

- Remote accessible interfaces/protocols.
- Trying to misuse (including brute force) SSH, Web GUI interface
- Performing generic IP fuzzing
- Trying to disrupt audit records (by remote means).

The total test effort expended by the evaluators in this re-evaluation was 8 days. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The developer tested the TOE in a stretched cluster configuration using the TOE models of HXAF220C-M5SX. The below diagram shows an overview of the TOE test configuration that was used by the developer and evaluator for both the original evaluation and this re-evaluation:

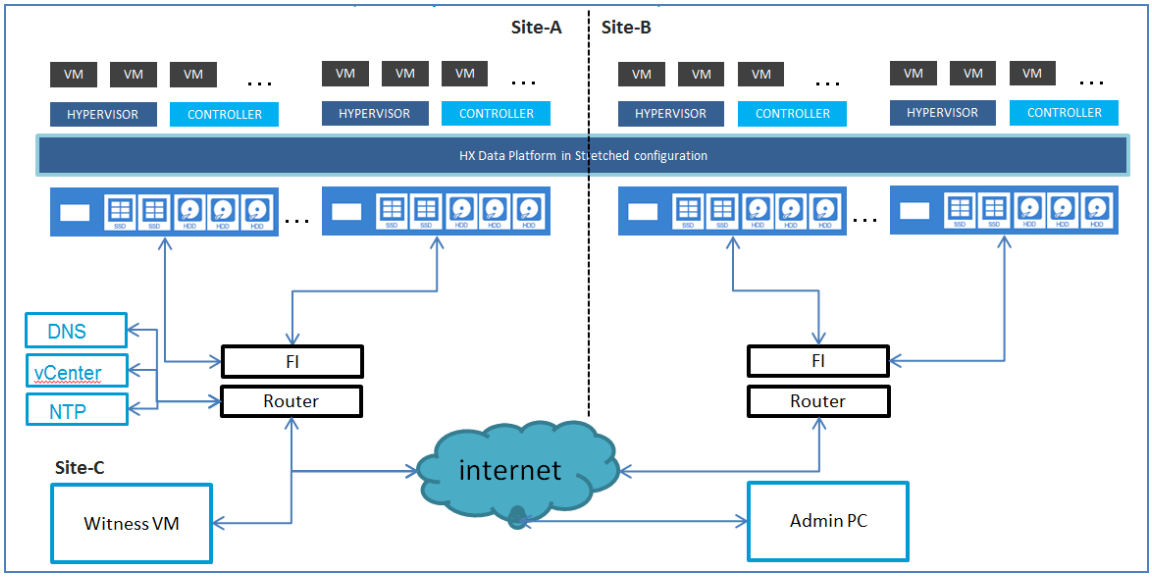

Figure 2 TOE test configuration overview (Site A, Site-B, and Site-C are located in the same location).

The evaluators examined the differences in the hardware and determined they were not security relevant and the enforcement of the security functional requirements is independent of the hardware differences. Therefore, it was concluded that the above test configuration is representative of the TOE as described in the *[ST]*.

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

This is a re-certification. Documentary evaluation results of the earlier version of the TOE have been reused, but vulnerability analysis and penetration testing has been renewed.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Cisco HyperFlex 4.5(2a) Systems HX Series.

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 Cisco HyperFlex 4.5(2a) Systems HX Series, to be **CC Part 2 conformant, 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]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” 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. Please note that the documents contain relevant details concerning the resistance against certain attacks.

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 user should pay particular attention to the use of whitelist access controls for this TOE, as detailed in [AGD] Table 2 “Terminology”. The whitelist access is configured during installation, and cannot be modified once the TOE is operational.

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 Cisco HyperFlex 4.5 Systems HX Series Common Criteria Security Target, Version: 3.0, 22 December 2021 *[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:

HDD	Hard-disk drives
HX	HyperFlex
HXCLI	HyperFlex Command Line Interface
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
SSD	Solid-state disk
TOE	Target of Evaluation
VMs	Virtual Machines

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]	Cisco HyperFlex 4.5 Systems HX Series - Evaluation Technical Report EAL2, 21-RPT-608, Version 3.0, 10 January 2022
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Cisco HyperFlex 4.5 Systems HX Series Common Criteria Security Target, Version: 3.0, 22 December 2021

(This is the end of this report.)