Certification Report

Cisco HyperFlex 3.5(2a) Systems HX Series

Sponsor and developer:	***Cisco Systems, Inc.*** **170 West Tasman Drive** **San Jose, CA 95134** **USA**
Evaluation facility:	***Brightsight*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-215885-CR**
Report version:	**1**
Project number:	**215885**
Author(s):	**Denise Cater**
Date:	**24 October 2019**
Number of pages:	**12**
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

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-19-215885**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

Cisco Systems Inc.

170 West Tasman Drive, San Jose, CA 95134, USA

Product and assurance level

Cisco HyperFlex 3.5(2a) Systems HX Series

Assurance Package:

- EAL2

Project number **215885**

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)

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.

Common Criteria Recognition Arrangement for components up to EAL2

INFORMATION TECHNOLOGY SECURITY SOGIS IT SECURITY CERTIFIED MUTUAL RECOGNITION AGREEMENT

SOGIS Mutual Recognition Agreement for components up to EAL4

Validity

Date of 1st issue : **25-11-2019**

Certificate expiry : **25-11-2024**

RvA 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

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.eIDAS-Regulation

TÜV Rheinland Nederland BV, operating the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), has been notified as a Designated Certification Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Cisco HyperFlex 3.5(2a) Systems HX Series. The developer of the Cisco HyperFlex 3.5(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, the Cisco HyperFlex 3.5 Systems HX Series, manages the storage of a storage cluster that has a minimum three servers HyperFlex HX Series Nodes with Solid-state disk (SSD) and Hard-disk drives (HDD) attached storage.

The HyperFlex HX Series installer is loaded on a UCS platform that is networked to the storage cluster to be managed. The HyperFlex HX Series includes HyperFlex Connect (HX Connect) GUI that 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 platform health, and manage resource use. Administrators can also use this data to predict when the cluster will need to be scaled.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 24 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 Cisco HyperFlex 3.5(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 3.5(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 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 HyperFlex 3.5(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 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	3.5(2a)

To ensure secure usage a set of guidance documents is provided together with the Cisco HyperFlex 3.5(2a) Systems HX Series. Details can be found in section “Documentation” of this report.

2.2 Security Policy

The TOE is comprised of the following security features:

- 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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

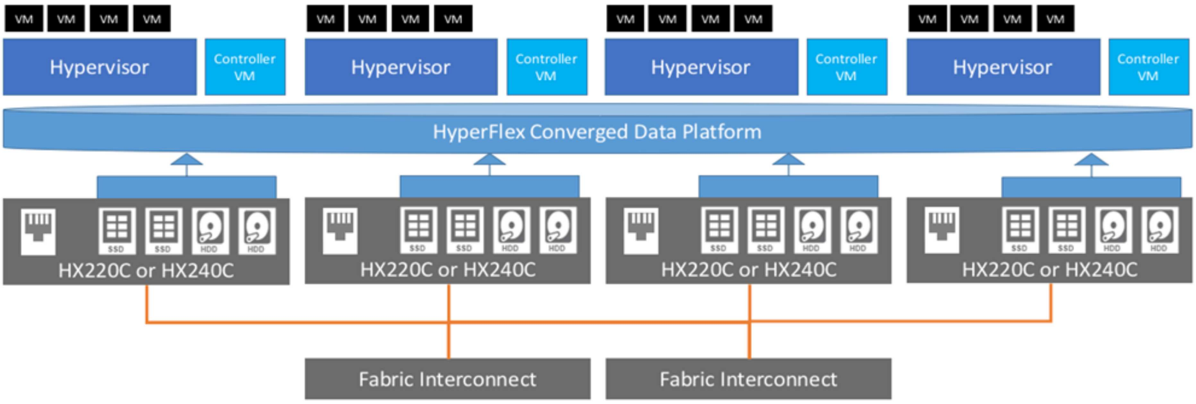
2.3.2 Clarification of scope

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

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:



2.5 *Documentation*

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

Identifier	Version
Cisco HyperFlex Systems HX Series Common Criteria Operational User Guidance and Preparative Procedures	Version 1.0, dated 7 October 2019

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. 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. Also, verifying that the user guidance provides all the necessary steps. As a result, the evaluators repeated the test cases for three (3) of the seven (7) TSFI. In addition to the developer tests, the evaluator derived and executed twelve (12) additional functional tests.

2.6.2 Independent Penetration Testing

To identify potential vulnerabilities the evaluator performed the following activities:

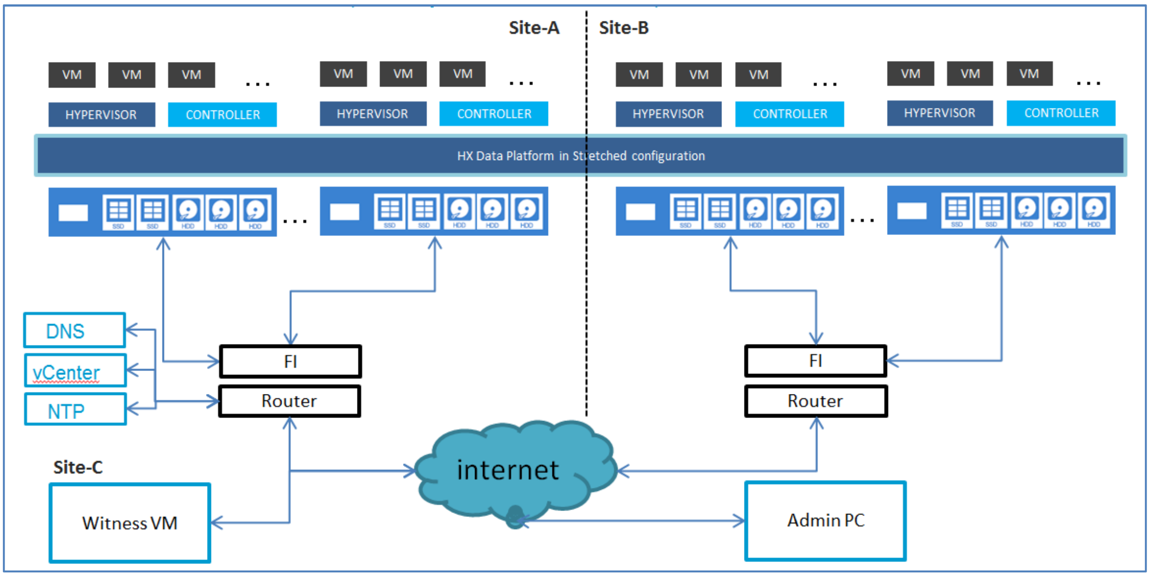
- SFR design analysis: Based on the information obtained in the evaluation evidence, the SFR implementation details were examined. The aspects described in CEM annex B were considered. During this examination several potential vulnerabilities were identified.
- Additional security analysis: When the implementation of the SFR was understood, a coverage check were 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 analyzed, 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.

The evaluator focused on the following, from which a total of nine (9) penetration tests were identified:

- 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).

2.6.3 Test Configuration

The TOE was tested by both the developer and evaluator in a stretched cluster configuration, using the TOE model HXAF220C-M5SX. The below diagram shows an overview of the test configuration used to test the TOE.



Note that for the purposes of testing, Site-A, Site-B, and Site-C are located in the same location.

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 HyperFlex 3.5(2a) Systems HX Series.

2.8 Results of the Evaluation

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 3.5(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]*.

2.9 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.

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 user should pay particular attention to the use of whitelist access controls for this TOE, as detailed in [AGD] section 3.6. 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. 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.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation.

3 Security Target

The Cisco HyperFlex 3.5 Systems HX Series Common Criteria Security Target, Version 1.0, 7 October 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
SSH	Secure Shell
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
[ETR]	Evaluation Technical Report Cisco HyperFlex 3.5(2a) Systems HX Series, 19-RPT-715, Version 2.0, 22 October 2019.
[NSCIB]	[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September April 2017.
[ST]	Cisco HyperFlex 3.5 Systems HX Series Common Criteria Security Target, Version 1.0, 7 October 2019.

(This is the end of this report).