

Certification Report

Cisco Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series running IOS-XR, version 7.4.1

Sponsor and developer: **Cisco Systems Inc.**
7025-2 Kit Creek Rd.
Morrisville, NC 27560
US

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

Report number: **NSCIB-CC-0597525-CR**

Report version: **1**

Project number: **0597525**

Author(s): **Brian Smithson**

Date: **21 April 2023**

Number of pages: **15**

Number of appendices: **0**

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

CONTENTS

Foreword	3
Recognition of the Certificate	4
International recognition	4
European recognition	4
1 Executive Summary	5
2 Certification Results	6
2.1 Identification of Target of Evaluation	6
2.2 Security Policy	6
2.2.1 Security Audit	6
2.2.2 User Data Protection	6
2.2.3 Identification and Authentication	6
2.2.4 Security Management	6
2.2.5 Protection of the TSF	7
2.2.6 TOE Access	7
2.2.7 Trusted Path/Channels	7
2.3 Assumptions and Clarification of Scope	7
2.3.1 Assumptions	7
2.3.2 Clarification of scope	7
2.4 Architectural Information	8
2.4.1 Logical architecture	8
2.4.2 Physical architecture	8
2.5 Documentation	9
2.6 IT Product Testing	9
2.6.1 Testing approach and depth	9
2.6.2 Independent penetration testing	10
2.6.3 Test configuration	10
2.6.4 Test results	11
2.7 Reused Evaluation Results	11
2.8 Evaluated Configuration	11
2.9 Evaluation Results	12
2.10 Comments/Recommendations	12
3 Security Target	13
4 Definitions	13
5 Bibliography	15

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 Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series running IOS-XR, version 7.4.1. The developer of the Cisco Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series running IOS-XR, version 7.4.1 is Cisco Systems Inc. located in Morrisville NC, US 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 the Cisco Network Convergence System 540, 5500 and 5700 Series (herein after also referred to as Cisco NCS or TOE). The TOE is a purpose-built, routing platform that is designed for redundancy, segment routing, programmable network management and primarily used for Wide Area Network (WAN) aggregation.

The Cisco NCS 540 includes small and medium density routers. The Cisco NCS5500 is a high-capacity modular routing series that is designed for redundancy, segment routing, programmable network management and primarily used for WAN aggregation. The Cisco NCS5700 Series Routers are designed for delivery of next-generation networking services, available in a 3-rack-unit compact chassis along with the Modular Port Adapters (MPAs) providing interfaces ranging from 1GE to 400GE.

All of the NCS routers run Cisco IOS-XR 7.4.1, a distributed microkernel-based network operating system.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 21 April 2023 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 Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series running IOS-XR, version 7.4.1, 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 Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series running IOS-XR, version 7.4.1 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.

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 Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series running IOS-XR, version 7.4.1 from Cisco Systems Inc. located in Morrisville NC, US.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	N540X-8Z16G-SYS-D N540X-8Z16G-SYS-A N540X-16Z4G8Q2C-D N540X-16Z4G8Q2C-A NCS-5504-SYS NC55-32T16Q4H-A (line card for the NCS-5504-SYS) NCS-57C3-MOD-SYS	N/A
Software	Cisco IOS-XR	7.4.1

To ensure secure usage a set of guidance documents is provided, together with the Cisco Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series running IOS-XR, version 7.4.1. For details, see section 2.5 "Documentation" of this report.

2.2 Security Policy

2.2.1 Security Audit

The TOE generates audit messages that identify specific TOE operations and provides an interface available for the Authorized Administrator to delete audit data stored locally on the TOE to manage the audit log space. The logs can be viewed on the TOE using the CLI interfaces.

2.2.2 User Data Protection

The TOE provides the ability to control traffic flow into or out of the Cisco NCS routers. The following types of traffic flow are controlled for both IPv4 and IPv6 traffic:

- Layer 3 Traffic – ACLs
- Layer 2 Traffic – Layer 2 Access Control Lists
- Virtual Routing and Forwarding - VRFs

2.2.3 Identification and Authentication

The TOE performs user authentication for the Authorized Administrator of the TOE and device level authentication. The TOE requires Authorized Administrators to authenticate with username and password prior to being granted access to any of the management functionality.

2.2.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All CLI TOE administration occurs either through SSHv2 secure connection or a direct local console connection. The TOE provides the ability to securely manage:

- Administer the TOE remotely
- Manage audit functionality

- Manage Information Flow Control Policies and Rules
- Manage Authorized Administrator's security attributes
- Review audit record logs
- Configure and manage the system time
- Maintain the system

2.2.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification and authentication, and limits configuration to the Authorized Administrator. Additionally, Cisco IOS-XR is not a general-purpose operating system and access to memory space is restricted to only IOS-XR functions. The TOE provides Information Flow Control Policies and Rules to ensure routing protocol communications between the TOE and neighbour switches is logically isolated from traffic.

2.2.6 TOE Access

The TOE enforces the termination of inactive sessions after an Authorized Administrator configurable time-period has expired. Once a session has been terminated, the TOE requires the Authorized Administrator to re-authenticate to establish a new session.

2.2.7 Trusted Path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 for remote CLI 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 3.1 of the [ST].

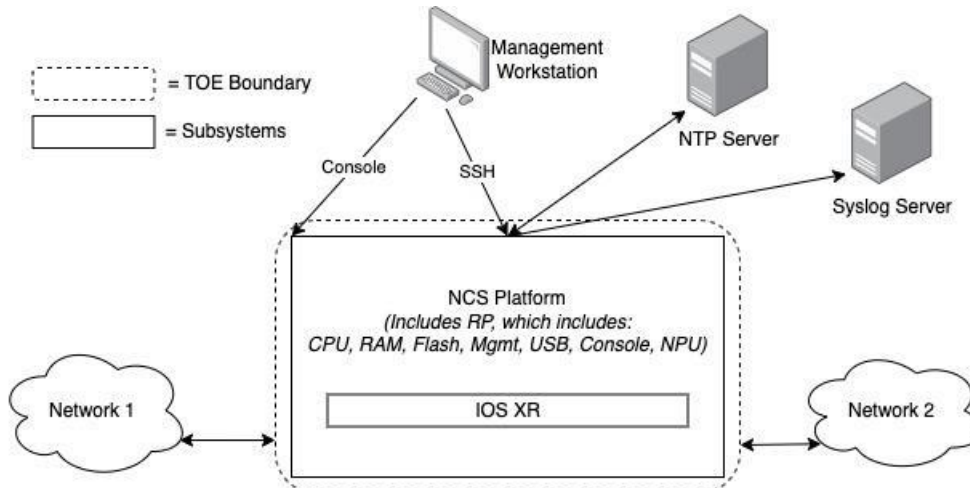
2.3.2 Clarification of scope

None.

2.4 Architectural Information

2.4.1 Logical architecture




The logical architecture, originating from the design of the TOE can be depicted as follows:

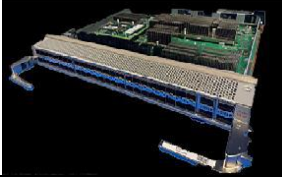



The non-TOE NTP and Syslog servers are not required. A non-TOE Management Workstation is mandatory.

2.4.2 Physical architecture

The physical specifications of NCS models under evaluation are summarized in the table below:

Model	Description	Processor	Interfaces
NCS540			
N540X-8Z16G-SYS-D N540X-8Z16G-SYS-A 	4-core 2GHz CPU 8 GB DRAM 16 GB eMMC 1 + 1 Fixed redundant DC 1 + 1 Fixed redundant AC Usable Rack Space: 1 RU	Marvell Cortex-A72 Armv8	8x 10/1GE 4x 1GE SFP 4x 1GE RJ45 8x 1GE SFP or 16x 1GE cSFP
N540X-16Z4G8Q2C-D N540X-16Z4G8Q2C-A 	8-core 1.7GHz x86 CPU 8GB DRAM 32GB storage Fixed dual redundant DC Modular Fan Tray with redundant fans Usable Rack Space: 1 RU	Intel Atom C3708 (Goldmont)	4x 1GE RJ-45 (10/100M) 16x 1GE/10GE 8x 1GE/10GE/25GE 2x 40GE/100GE
NCS5500			
NCS-5504-SYS 	Supports up to 4 line cards, 6 switch fabric cards, 2 route processors, 2 system controllers, 3 fan trays, 4 power supplies (AC or DC). Usable Rack Space: 7RU	Intel Xeon D-1528 (Broadwell)	Based on route processors and line-cards installed. For this evaluation: NC55-32T16Q4H-A

Model	Description	Processor	Interfaces
NC55-32T16Q4H-A 	2 x 10GE SFP+, 16 x 25GE SFP28 and 4x 100GE QSFP28 ports, 1 forwarding ASIC.		2 x 10GE SFP+ 16 x 25GE SFP28 4x 100GE QSFP28
NCS5700			
NCS-57C3-MOD-SYS 	8 cores at 2 GHz 32GB DRAM 256GB Flash 2 hot-swappable power supplies provide 1 + 1 redundancy Front-to-back airflow 6 hot-swappable fan trays provide 5 + 1 redundant system cooling Usable Rack Space: 3RU	Intel Xeon D-1563N (Broadwell)	1 USB RJ-45 Console Management Ethernet Fixed 48x 1/10/25G 8x 100G 3x MPA Base Chassis

2.5 Documentation

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

Identifier	Version
Cisco Network Convergence System 540, 5500 and 5700 Series Common Criteria Operational User Guidance and Preparative Procedures (EDCS: 23191545)	v1.1 23rd March 2023

2.6 IT Product 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

As the TOE type belongs to the networking products, [NSI#08] permits tests to be performed remotely. Since the tests are performed remotely, it is not in scope of ISO17025.

The developer enabled the evaluator to directly control the TOE as well as it’s environment to ensure the tests are performed on the correct TOE with correct supporting environment. A WebEX link was set up to share the control of the testing PC at the developer’s premises so the evaluator could directly operate the TOE and its environment via WebEX. The developer also provided full support during the testing. The evaluator remained responsible for installing and configuring the TOE within the test environment by performing a various control mechanisms including verifying the TOE hardware models and installation with photos, and verifying the TOE software by checking the version and the hash value of the TOE software image installed on the hardware. The evaluator also performed AGD_PRE activities to ensure the TOE is configured in the certified configuration.

The models in scope include fixed and modular chassis router of different size (RUs) and number of ports. The differences are non-security relevant (computing power, interface type, memory size, power supplies). All devices run the same software Cisco IOS-XR 7.4.1, all devices claim the same security functionality, and none claims additional functionality.

To eliminate any possibility for potential discrepancy across the different TOE models, all models have been sampled for testing, either in developer tests or evaluator tests. However, some differences in behavior among models were discovered during testing, and the relevant tests were repeated on all models.

The developer provided test plans for each NCS model sampled for developer testing, consisting of seven (7) test cases which cover the functionality claimed in the ST. As all SFRs are tested, all the TSFIs are also tested. The repeated developer tests considered verification of SSH (as it is remotely accessible), verification of user identification and role-based privileges, and verification of flow control enforcement.

The evaluator created twelve (12) additional test cases test to confirm verification of the version of the TOE, to supplement coverage of SFRs and/or TSFI, and to further exercise the behaviour of critical functionality:

- Scanning to determine available services and potential undocumented ones.
- Tests that complement/extend the developer tests, such as negative tests for ACL configuration and verifying user roles and attributes.
- Testing certain claims mentioned in Security Architecture and AGD

2.6.2 Independent penetration testing

SFR implementation details were examined in the SFR design analysis. During this examination several potential vulnerabilities were identified:

- Using the CWE weaknesses collection, the evaluator collected a list of security questions and related answers. During this examination, several potential vulnerabilities were identified.
- The evaluator runs vulnerability scanning tools to identify potential vulnerabilities.
- Several additional potential vulnerabilities were identified during a search in the public domain.

Ultimately, ten (10) penetration tests were devised to verify that the TOE, in its operational environment is resistant to an attacker possessing a Basic attack potential.

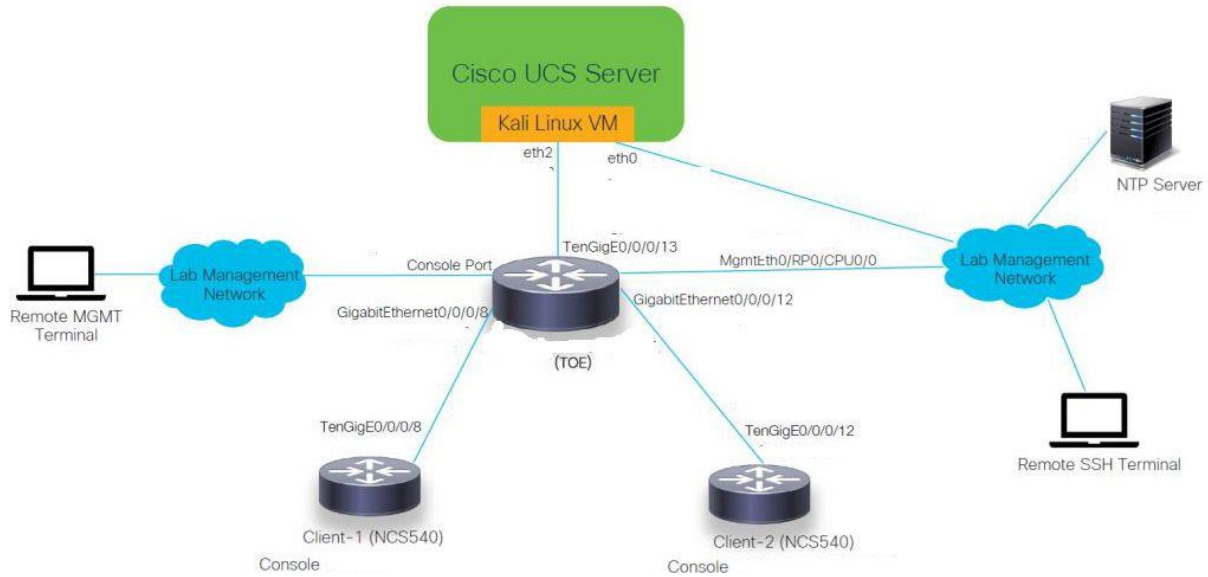
The total test effort expended by the evaluators was three (3) weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

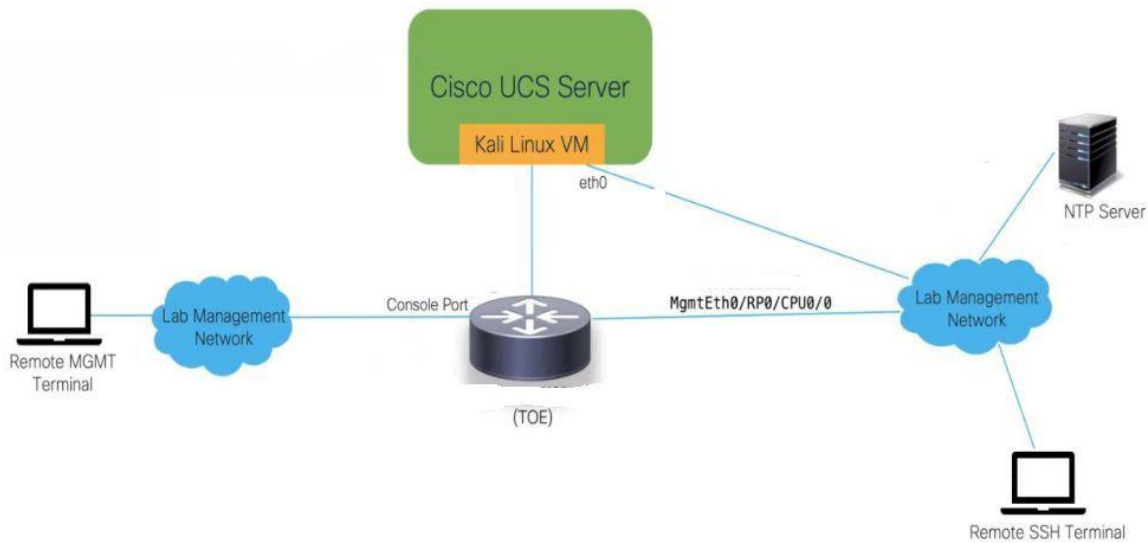
Tools used in the test environment:

Description	Package Name	Version
Operating system	Kali (Virtual machine)	6.0.0
Terminal	Linux terminal	n/a
Packet capture	Wireshark	4.0.1
Network enumeration	NMAP	7.93
IP stack integrity checker	isic	0.07
SSH client, key generation	PuTTY	0.78
SSH fuzzing	Metasploit	6.2.26-dev
Password bruteforce	Hydra	9.4
Vulnerability scan tool	Nessus	10.4.1 and 10.5.0

Configuration for NCS 540 (small formfactor) and NCS 5500:



Configuration for NCS 5700 and NCS 540 (medium formfactor):



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.

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 Cisco Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series running IOS-XR, version 7.4.1.

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 Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series running IOS-XR, version 7.4.1, 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>, which are out of scope as there are no security claims relating to these.

3 Security Target

The Cisco Network Convergence System 540, 5500 and 5700 Series Common Criteria Security Target, NCS_IOS-XR_7.4_EAL2_ST_v1.1, v1.1, 29 March 2023 [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:

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
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standards
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
FC	Fibre Channel
HDD	Hard-disk drives
IP	Internet Protocol
PACLs	Port Access Control List
OS	Operating System
RACLs	Receive Access Control List
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SM	Service Module
SSD	Solid-state disk
SSH	Secure Shell
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol

TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding
VSAN	Virtual Storage Area Network
XML	Extensible Markup Language
WAN	Wide Area Network

5 Bibliography

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

- [ADV-AGD ref] ADV-AGD reference document Cisco NCS 5xx 5xxx Series, 22-RPT-961, v1.0, 21 December 2022
- [AGD] Cisco Network Convergence System 540, 5500 and 5700 Series Common Criteria Operational User Guidance and Preparative Procedures, EDCS: 23191545, v1.1, 23 March 2023
- [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 NCS EAL2+, 22-RPT-965, v1.0, 29 March 2023
- [IR ADV] Cisco NCS 540 5500 5700 Series, 22-RPT-960, v1.0, 21 December 2022
- [IR ALC] ALC presentation EAL 2+ Cisco Network Convergence, 22-RPT-962, v1.0, 21 December 2022
- [IR ASE] Cisco NCS EAL2+ IR ASE, 22-RPT-966, v2.0, 16 December 2022
- [IR-ATE_AVA] Cisco NCS 540 5500 5700 Series Presentation, 22-RPT-963, v2.0, 29 March 2023
- [NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
- [NSI#08] NSCIB Scheme Instruction 08 – Performing Testing, v2.7, 6 August 2021
- [ST] Cisco Network Convergence System 540, 5500 and 5700 Series Common Criteria Security Target, NCS_IOS-XR_7.4_EAL2_ST_v1.1, v1.1, 29 March 2023
- [TEST_PLAN] ATE and AVA Test Report, 22-RPT-964, v2.0, 29 March 2023

(This is the end of this report.)