EUCC Certification Report

Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11

Sponsor and developer:	***Cisco Systems, Inc.*** **170 West Tasman Drive** **95134 San Jose, CA** **USA**
Evaluation facility:	***Applus+ Laboratories*** **Av. de Aragón, 402, Edificio Allende – 5ª planta Applus** **28022 San Blas Cannillejas (Madrid)** **Spain**
Report number:	**EUCC-3110-2026-2500100-01 Certification Report**
Report version:	**1**
Project number:	**EUCC-2500100-01**
Author(s):	**Wim Ton, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**28 April 2026**
Number of pages:	**16**
Number of appendices:	**0**

CONTENTS

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated 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 security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the ICT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the ICT product satisfies the security requirements stated in the security target.

International recognition of the certificate

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of published 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.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11, (ASR9K), identified in this document as either the ICT Product or as the Target of Evaluation (TOE).

The developer of the ICT Product is Cisco Systems, Inc. located in San Jose, USA and they also act as the sponsor of the evaluation.

This Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the ICT product for their particular requirements.

The ASR9K is a scalable carrier-class router, which is designed for redundancy, high security and availability, packaging, power, and other requirements needed by service providers. The ASR9K is designed to provide continuous system operation, scalability, security, and high performance.

The ASR9K runs IOS-XR that is a microkernel-based network operating system. IOS-XR is able to process data as it comes into the router without buffering delays. The microkernel is responsible for specific functions such as memory management, interrupt handling, scheduling, task switching, synchronization, and inter-process communication. The microkernel's functions do not include other system services such as device drivers, file system, and network stacks; those services are implemented as independent processes outside the kernel, and they can be restarted like any other application.

The TOE versions differ in the number and type of the network connections and the processing capacity. They are all based on the same processor family, Intel Xeon and all run the same software.

The TOE claims conformance to the following Protection Profile *[PP]*:

- collaborative Protection Profile for Network Devices 3.0e 6 December 2023, with Functional Package for Secure Shell (SSH) 1.0 13 May 2021,

A certification procedure was conducted on the TOE by TrustCB B.V., in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024 and (EU) 2025/2462 of 8 December 2025.

The successful completion of the certification procedure resulted in TrustCB issuing an EUCC certificate, The certificate identifier is **EUCC-3110-2026-2500100-01**, dated 28-04-2026 and with a 5-year validity.

The evaluation of the TOE was performed by Applus+ Laboratories located in Barcelona, Spain. The evaluation was completed on 28-04-2026 with the issuance of the evaluation technical report *[ETR]*. The evaluation was conducted using the Common Criteria Evaluation Methodology for Information Security Evaluation, CCv3.1 revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC3.1 Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5. *[CC]*.

The scope of the evaluation was defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the ICT Product, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

The results documented in the evaluation technical report [ETR] for this product provide sufficient evidence that the TOE meets the requirements for exact conformance to the collaborative Protection Profile for Network Devices [PP], referencing specific assurance packages ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE.REQ.1, ASE.TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1 and ALC_FLR.2.

This assurance level is recognised by article 52 of [CSA] as ‘substantial’.

Consumers of this ICT Product 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.

TrustCB B.V., as Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates.

Note that the certification results apply only to the specific version of the product as evaluated.

2 ICT Product details

2.1 Identification of the ICT Product

The Target of Evaluation (TOE) for this evaluation is ICT product Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11 (ASR9K) from Cisco Systems, Inc. located in San Jose, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Chassis	ASR-9006-SYS
		ASR-9010-SYS
		ASR-9902
		ASR-9903
		ASR-9904
		ASR-9906
		ASR-9910
		ASR-9912
		ASR-9922
	Route Processors	A99-RP3
		A9K-RSP5
		A99-RP3-X
		A9K-RSP5-X
		A99-RP-F
	Line Cards	A99-4HG-FL
		A9K-4HG-FLEX
		A9K-8HG-FLEX
		A9K-20HG-FLEX
		A99-10X400GE-X
		A99-4T
		A9903-8HG-PEC
		A9903-20HG-PEC
		A99-32X100GE-X
		A99-32HG
Software	Cisco IOS-XR	7.11

Additional requirements for the operational environment of the certified ICT product are described in section 3.1 of the *[ST]*.

To ensure secure usage a set of guidance documents is provided with the TOE. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information.

2.2 Contact information related to the evaluation of the ICT Product

Holder of the EUCC Certificate

Organisation name:	Cisco Systems, Inc.
Address:	170 West Tasman Drive, 95134 San Jose, CA USA
Certified product contact details	certteam@cisco.com

Developer of the certified ICT Product

ICT product developer	Cisco Systems, Inc.

Identification of CAB

The Certification Assessment Body for this ICT Product is TrustCB B.V. TrustCB is licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC certification activities up to and including EUCC High.

TrustCB point of contact: EUCC@trustcb.com

Identification of ITSEF

Evaluation and testing for this ICT Product was performed by following ITSEF:

Applus+ Laboratories in Barcelona, Spain

2.3 Security services and policies

2.3.1 Security services

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;
- Cryptographic Support;
- Identification and Authentication;
- Security Management;
- Protection of the TSF;
- TOE Access;
- Trusted Path/Channels.

2.3.2 Vulnerability management

The following vulnerability policy has been identified as applicable to the Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11

Document reference: Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11 Life-Cycle Support Vulnerability Management and Disclosure (EUCC), Version 1.0, 15 Apr 2025

2.3.3 Assurance Continuity policies

This is a new product certification. An assurance continuity policy was not provided.

2.3.4 Lifecycle management processes and production facilities

Not applicable to this evaluation

2.3.5 Patch management process

Not applicable to this evaluation

2.4 Assumptions and Clarification of Scope

2.4.1 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]*.

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions described in the [ST].

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 concerning the resistance against certain attacks.

2.4.2 Clarification of scope

Threats addressed by the TOE and the IT environment are presented in Section 3.2 of *[ST]* and include the threats as presented in the *[PP].* No items have been added, removed or modified for the TOE. The assumed level of expertise of the attacker for all identified threats is Basic.

The Organizational Security Polices (OSPs) are the same as in *[PP]*. No OSPs have been added, removed or modified

2.5 Architectural Information

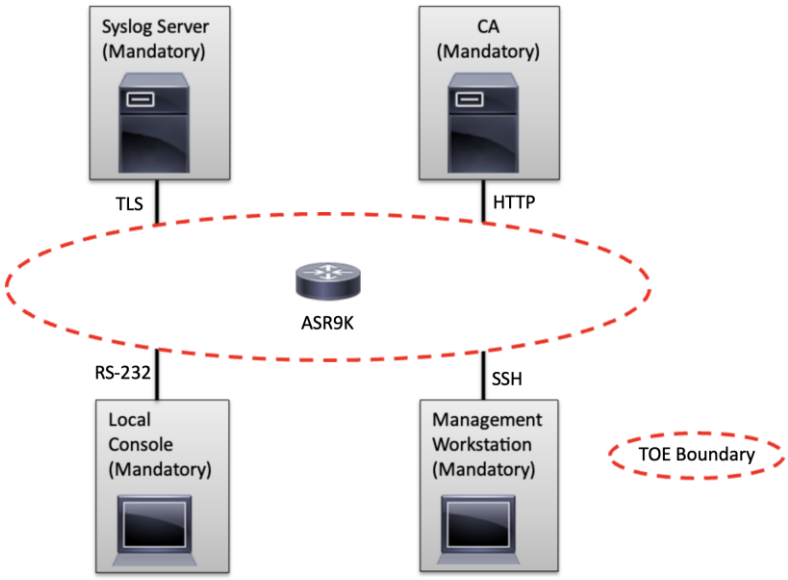


Figure 1 The TOE in its environment

2.6 Supplementary Cybersecurity Information

The following website link was provided for the Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11 for the supplementary cybersecurity information referred to in Article 55 of Regulation (EU) 2019/881:

https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html

This link provides further details and links on:

- Guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11.
- The period during which the Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11 security support will be offered to end users, in particular as regards the availability of

cybersecurity related updates, is stated as 5 years, aligned with the validity of the issued EUCC certificate).

- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11.
- the online repository listing publicly disclosed vulnerabilities related to the Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11 and to any relevant cybersecurity advisories .

Note: The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11:

Identifier	**Version**
Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11 Common Criteria Operational User Guidance and Preparative Procedures	2.3
System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x	2023-11-30
Cisco ASR 9000 Series Aggregation Services Router Hardware Installation Guide	2021-03-30
Cisco ASR 9000 Series Fixed-Port Routers Hardware Installation Guide	2021-07-30

3 Evaluation summary

3.1 Identification of used assurance components

The assurance components used in the product testing were:

- **ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE.REQ.1, ASE.TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1 and ALC_FLR.2.**

as defined by, and detailed in, *[CC]* and *[CEM]*.

3.2 EUCC State of the Art documents and Protection Profiles

The following Protection Profile was applied:

Collaborative Protection Profile for Network Devices, v3.0e, 06 December 2023, with the Functional Package for Secure Shell (SSH), v1.0, 13 May, 2021,

3.3 ICT 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.

3.3.1 Testing approach and depth

The *[PP]* explicitly delegates the responsibility for testing to the evaluator, who must perform the evaluation activities as defined in the Evaluation Activities for Network Devices cPP. These activities are designed to independently verify the implementation of the Security Functional Requirements without relying on the developer's internal testing evidences.

3.3.2 Independent penetration testing

The evaluators used port scanning and fuzzing to check for residual vulnerabilities.

3.3.3 Test configuration

After analysing the differences between TOE models provided in (DAR_TRR_0.1), the evaluator concluded that all TOE hardware models were equivalent.
The evaluation team performed full testing on a Cisco ASR-9006 modular chassis having the following components:

- Route Processors:
  - A9K-RSP5-X-TR (Intel Xeon D-1573N)
- Line Cards:
  - A9K-4HG-FLEX-SE
  - A99-32X100GE-X-TR

3.3.4 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.

3.4 ICT Product evaluation

3.4.1 Reused evaluation results

There is no reuse of evaluation results in this certification.

3.4.2 Evaluated configuration

The TOE is defined uniquely by its name and version number Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11.The user can view the version with the “show version” command on the console. With the “show logging | fips” command, the user can view if the TOE is configured in “FIPS mode”, which is the certified configuration.

3.4.3 Assessment against each assurance requirement

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1
Security objectives	ASE_OBJ.1
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.1
TOE summary specification	ASE.TSS.1

The findings are well-documented and internally consistent, demonstrating a thorough understanding of the Security Target *[ST]* and its components. The TOE introduction, conformance claim, security problems, security objectives, security requirements, TOE summary specification are appropriately addressed, and the TOE description is accurate and adequate for the evaluation level. Consequently, the ASE activities fulfil the assurance requirements in the [PP] augmented with ALC_FLR.2. No issues or deviations were identified

ADV

ADV	
Functional specification	ADV_FSP.1

The evaluation has demonstrated that the developer’s evidence meets ADV specified requirements. The TOE model is complete, clearly showing all interfaces (TSFI/non-TSFI), user roles, and relations, with explanations on completeness and tracing requirements met. Accordingly, the ADV activities meet the assurance requirements in the [PP] augmented with ALC_FLR.2, with no issues or deviations identified

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure acceptance, installation, configuration, and operation of the TOE within its intended environment by its user roles. The guidance effectively helps prevent common misconfigurations and promotes correct usage. Therefore, the AGD activities fulfil the assurance requirements in the [PP] augmented with ALC_FLR.2, with no issues or deviations identified.

ALC

ALC	
CM capabilities	ALC_CMC.1
CM Scope	ALC_CMS.1

Flaw remediation	ALC_FLR.2

The evaluation has demonstrated that the developer's evidence meets ALC specified. The CI-list was comprehensive and uniquely identified all configuration items, with clear identification of the developer. The CM documentation effectively described unique identification methods, a CM plan for development, procedures for accepting modified or new CIs, and the CM system was operated in accordance with the CM plan to maintain all configuration items by automated means. Flaw remediation procedures were comprehensive, including methods for receiving reports, tracking flaws, providing corrective actions, and updating users. Accordingly, the ALC activities satisfy the assurance requirements in the [PP] augmented with ALC_FLR.2, with no issues or deviations identified.

.**ATE**

ATE	
Independent testing	ATE_IND.1

For the evaluator's independent testing, the overall approach for test selection, goals for the witnessing session, and independent test plan were clearly outlined. The evaluator's testing results showed that all sampled tests were passed. Accordingly, the ATE activities satisfy the assurance requirements in the [PP] augmented with ALC_FLR.2, with no issues or deviations identified.

AVA

AVA	
Vulnerability analysis	AVA_VAN.1

The evaluator conducted a public domain vulnerability search. Additionally, the evaluator executed a number of tests using scanning tools to verify if new potential vulnerabilities could impact any of the services running on the TOE in the evaluated configuration, fuzzing tests on the network interfaces and privilege escalation on the CLI.

Consequently, the AVA activities were performed in full compliance with the assurance requirements in the [PP] augmented with ALC_FLR.2, providing a substantial level of confidence in the TOE's resistance to exploitation.

3.5 Results of the evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report, other evaluator documents and developer documentation *[DEV_DOCS]*.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the evaluation results the evaluation lab concluded the Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11, to be **Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5 conformant** at an assurance level recognised by article 52 of [CSA] as ''**Substantial**' with the assurance packages: ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.1, ASE_ECD.1, ASE.REQ.1, ASE.TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1 and ALC_FLR.2. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

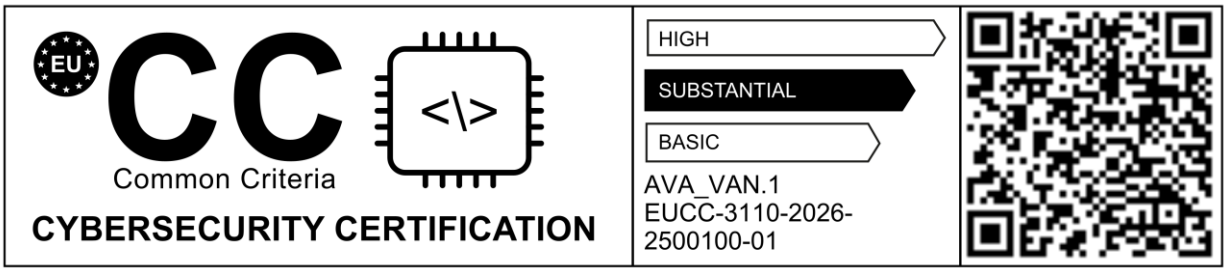
The Security Target claims 'exact' conformance to the Protection Profile *[PP]*.

3.6 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-3110-2026-2500100-01

Date of issuance: 28-04-2026 and with a validity period of **5 years**.



3.7 Comments and Recommendations

The user guidance as outlined in section 2.6 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 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 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.

4 Security Target

The certification references the following security target:

Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11 Security Target, v2.5, 10 March 2026 *[ST]*.

5 Glossary

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information and communication technologies product as defined by [EUCC]
ITSEF	IT Security Evaluation Facility
EUCC	European Cybersecurity Certification Scheme [EU-EUCC], created under the Cybersecurity Act [EU-CSA] and detailed in Commission Implementing Regulation (EU) 2024/482
PP	Protection Profile
SotA	EUCC State-of-the-Art document
TOE	Target of Evaluation; the object of the certification activity described by this report
ACL	Access Control List
AES	Advanced Encryption Standard
CA	Certification Authority
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
JIL	Joint Interpretation Library
LAN	Local Area Network
PKI	Public Key Infrastructure
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VLAN	Virtual LAN

6 Bibliography

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

[CC]	ISO/IEC 15408-1 :2009, -2 :2008, -3 :2008, Common Criteria for Information Technology Security Evaluation (CC) version 3.1 revision 5, April 2017
[CEM]	ISO/IEC 18045 :2008, Common Criteria Evaluation Methodology for Information Security Evaluation (CEM) version 3.1 revision 5, April 2017
[DEV_DOCS]	Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11 Common Criteria Operational User Guidance and Preparative Procedures v2.3 System Security Configuration Guide for Cisco ASR 9000 Series Routers, IOS XR Release 7.11.x, 30 November 2023 Cisco ASR 9000 Series Aggregation Services Router Hardware Installation Guide, 30 March 2021 Cisco ASR 9000 Series Fixed-Port Routers Hardware Installation Guide, 30 July 2021 Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11 Configuration Item List, v1.0, 8 April 2026
[ETR]	Evaluation Technical Report, CNLCIS001, Version M0, 28 April 2026
[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[EU-EUCC-amdt.1]	Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 amending Implementing Regulation (EU) 2024/482 as regards applicable international standards and correcting that Implementing Regulation
[EU-EUCC-amdt.2]	Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025 amending Implementing Regulation (EU) 2024/482 as regards definitions, ICT product series certification, assurance continuity and state-of-the-art documents
[PP]	collaborative Protection Profile for Network Devices, version 3.0e dated 06 December 2023, validated under NIAP 25 April 2024
[CPP_ND_SD_V3.0E]	Evaluation Activities for Network Device cPP, v3.0e, 06 December, 2023
[PKG_SSH]	Functional Package for Secure Shell (SSH), v1.0, 13 May, 2021
[ST]	Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11 Security Target, v2.5, 10 March 2026

(This is the end of this report.)