Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Nokia IXR Service Router Linux (SR Linux) Family v24.10.4

15 December 2025

655-EWA

v1.0

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Program, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

This report, and its associated certificate, are not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Program provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCTL.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Nokia IXR Service Router Linux (SR Linux) Family v24.10.4 (hereafter referred to as the Target of Evaluation, or TOE), from **Nokia Corporation** , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

EWA-Canada is the CCTL that conducted the evaluation. This evaluation was completed on **15 December 2025** and was carried out in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Nokia IXR Service Router Linux (SR Linux) Family v24.10.4
Developer	Nokia Corporation

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

EAL 3+ (ALC_FLR.1)

1.2 TOE DESCRIPTION

The TOE is a network operating system (NOS) router/switch providing network operating system functionality.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

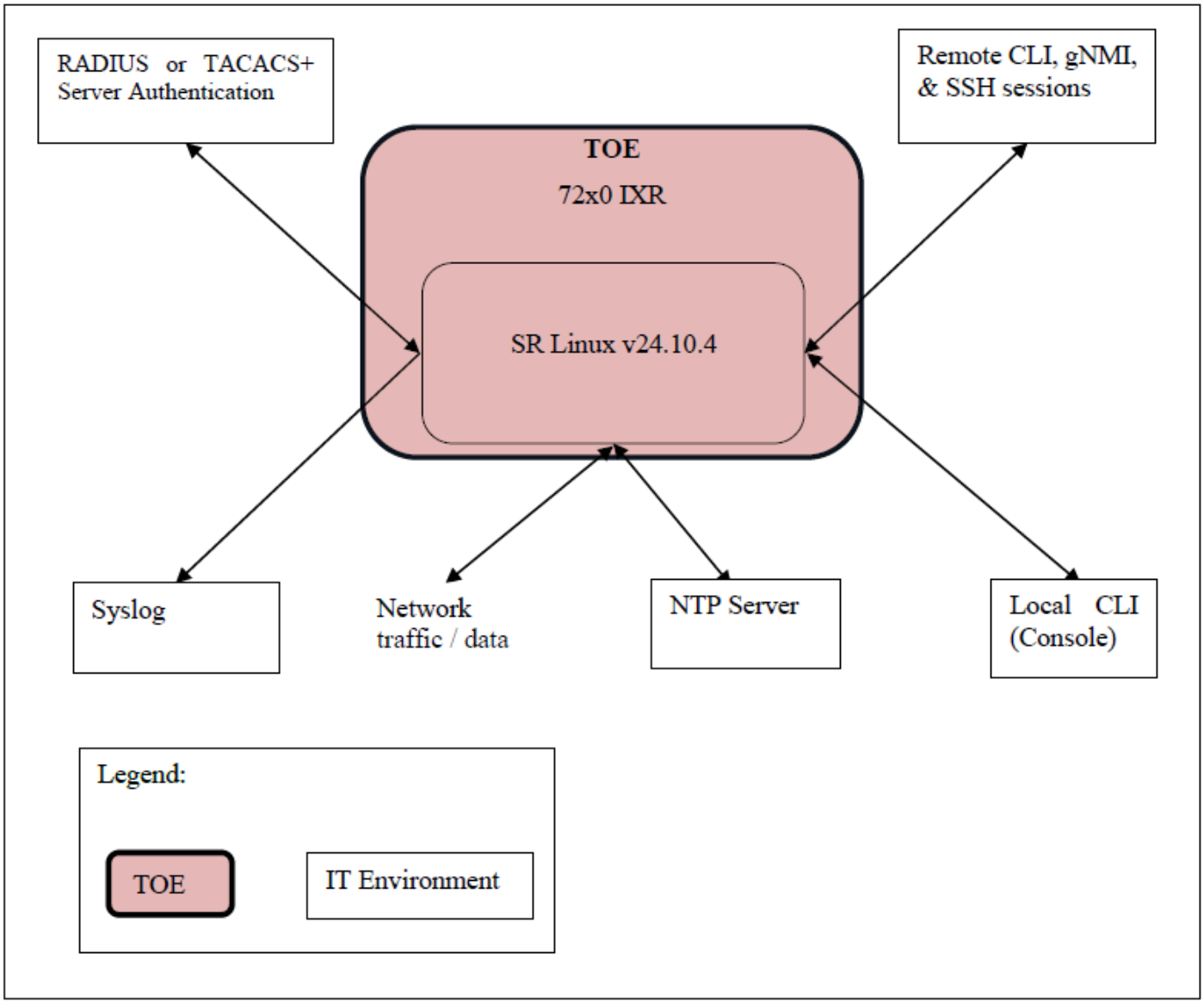

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementation are used by the TOE and have been evaluated by the CAVP:

Table 2: Cryptographic Implementation

Cryptographic Implementation	Certificate Number
Nokia SR Linux Cryptographic module (SRLCM) v24.10.4	A7218

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- Authorized administrators are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance, and will periodically check the audit record; however, they are capable of error. It is further assumed that personnel will be trained in the appropriate use of the TOE to ensure security.
- External authentication services will be available to the TOE via either RADIUS, TACACS+, or both, based on defined Internet Engineering Task Force (IETF) standards.
- TOE functions with the external IT entities shown in Figure 1 and with other vendors' routers on the network and meets Request for Comments (RFC) requirements for implemented protocols.
- There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- The operational environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE. It is further assumed that the processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.
- The operational environment provides the TOE with the necessary reliable time stamp. External Network Time Protocol (NTP) services will also be available to provide external time synchronization.
- Trusted remote systems that communicate with the TOE, except for the network traffic/data interface, are attached to an internal trusted protected network that is only accessible by infrastructure devices and trusted administrators. This includes: (1) the RADIUS, TACACS+ server; (2) the Syslog servers; and (3) the NTP server.
- The Network traffic/data interface is attached to internal and external networks. Console Access is via RS-232, a direct local connection in the same physical location as the TOE.

3.2 CLARIFICATION OF SCOPE

The following features of the TOE are outside the evaluated configuration.

- The high availability (HA) feature is not in the scope of the evaluated configuration.
- The following protocols and technologies are not in the scope of the evaluated configuration.
    - Border Gateway Protocol (BGP)
    - MAC-VRF
    - Multiprotocol Label Switching (MPLS)
    - Label Distribution Protocol (LDP)
- Third-party developed applications that plug into the SR Linux framework.
    - CLI Plug-Ins
- gRPC Routing Information Base Interface (gRIBI) – a gRPC-based protocol that allows external applications to change routes in a device's routing information base (RIB).
- Packet capture filters that copy and extract packets for inspection by tools outside the TOE to protect against Distributed and other DoS (D/DoS) attacks.
- Filtering based on IP Differentiated Services Code Point (DSCP).

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software/Firmware	V24.10.4	
TOE Hardware	• 7220 IXR-D1 • 7220 IXR-D2 • 7220 IXR-D2L • 7220 IXR-D3 • 7220 IXR-D3L • 7220 IXR-D4 • 7220 IXR-D5	• 7220 IXR-H2 • 7220 IXR-H3 • 7220 IXR-H4 • 7250 IXR-6e • 7250 IXR-10e • 7250 IXR-X1b • 7250 IXR-X3b
Environmental Support	• RADIUS/TACACS+ Server • Syslog Server • NTP Server	

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 ACL and Policy-based Routing Guide, 3HE 20968 AAAA TQZZA,01, November 2024

b) Nokia Service Router Linux, 7220 Interconnect Router, 7250 Interconnect Router, Release 24.10 Advanced Solutions Guide, 3HE 20952 AAAA TQZZA, 01, November 2024

c) Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Configuration Basics Guide, 3HE 20951 AAAA TQZZA, 01, November 2024

d) Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Data Model Reference, 3HE 20958 AAAA TQZZA, 01, November 2024

e) Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Log Events Guide, 3HE 20957 AAAA TQZZA, 01, November 2024

f) Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Product Overview, 3HE 20948 AAAA TQZZA, 01, November 2024

g) Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Routing Protocol Guide, 3HE 20966 AAAA TQZZA, 01, November 2024

h) Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 Software Installation Guide, 3HE 20953 AAAA TQZZA, 01, November 2024

i) Nokia Service Router Linux, 7215 Interconnect System, 7220 Interconnect Router, 7250 Interconnect Router, 7730 Service Interconnect Router, Release 24.10 System Management Guide, 3HE 20949 AAAA TQZZA, 01, November 2024

j) Nokia IXR Service Router Linux (SR Linux) Family v24.10.4 Supplemental Common Criteria Guidance, 2233-002-D105, 1.0, 25 November 2025

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all the procedures required to maintain the integrity of the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT TESTING

During this evaluation, the evaluator developed independent functional & penetration tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests.

b. Cryptographic Implementation Verification: The evaluator verified that the claimed cryptographic implementation was present in the TOE.

c. Cipher Suite Verification: The evaluator verified that the TOE supports the claimed cipher suites.

d. Authentication Method Verification: The evaluator verified that the TOE supports the claimed authentication methods.

e. Trusted Path Verification: The evaluator verified that the TOE provides a trusted path between itself and remote entities.

f. Network Traffic Filtering: The evaluator verified that the TOE could filter traffic.

6.3.1 INDEPENDENT TESTING RESULTS

The developer's tests and the independent tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 VULNERABILITY ANALYSIS

The vulnerability analysis focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their vulnerability analysis.

Type 1 & 2 searches were conducted on **5 November 2025** and included the following search terms:

TOE Name/Version (Section 4)	OpenSSL 3.0.15	OpenSSH 9.2p1
gNMI	Free Radius 3.0.19	

Vulnerability searches were conducted using the following sources:

NOKIA PSIRT https://www.nokia.com/about-us/security-and-privacy/product-security-advisory/	National Vulnerability Database https://nvd.nist.gov/vuln/search
CISA Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog	

6.4.1 VULNERABILITY ANALYSIS RESULTS

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

This evaluation has provided the basis for the conformance claim documented in Section 1.1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Evaluation Technical Report Nokia IXR Service Router Linux (SR Linux) Family v24.10.4, 2025-12-15, v1.3.
Security Target Nokia IXR Service Router Linux (SR Linux) Family v24.10.4, 2025-11-25, v1.0.