ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Nokia 7x50 SR OS 20.10.R12 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e

Maintenance Update of Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e

Maintenance Report Number: CCEVS-VR-VID11183-2023

Date of Activity: October 19, 2023

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008.
- Nokia 7x50 SR OS 20.10.R12 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e Impact Analysis Report for Common Criteria Assurance Maintenance Update from Version Nokia SR OS 20.10.R4 to Version Nokia SR OS 20.10.R12
- Collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]

Documentation updates

Evidence Identification	Effect on Evidence/ Description of Changes
Security Target: Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e Security Target, Version 3.0, October 12, 2021	**Maintained Security Target:** Nokia 7x50 SR OS 20.10.R12 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e Security Target, version 3.1, May 30, 2023 Changes in the maintained ST are: • Version number of TOE changed from • Nokia 7x50 SR OS 20.10.R4 to Nokia 7x50 SR OS 20.10.R12 • Updated the TOE documentation references.

Common Criteria Guidance Documentation	**Maintained Common Criteria Guidance documentation:**
• Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e Guidance Document, Version 0.7, October 12,2021	• Nokia 7x50 SR OS 20.10.R12 for 7750 SR-1, 7750 SR-1s, 7750 SR-2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e Guidance Document, Version 0.8, May 30, 2023 Changes in the maintained Guidance are: • Version number of TOE changed from Nokia 7x50 SR OS 20.10.R4 to Nokia 7x50 SR OS 20.10.R12 • All the changes documented in this report corresponding to the updates to the TOE.

Assurance Continuity Maintenance Report

Nokia Corporation submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on June 9,2023. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0. In accordance with those requirements, the IAR describes the changes made to the maintained TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence consists of the Security Target, guidance documentation, vulnerability analysis and the Impact Analysis Report (IAR) . The ST, guidance documentation and vulnerability analysis were updated, the IAR documented the changes from the previous version of the TOE (Nokia 7x50 SR OS 20.10.R4) to the updated TOE(Nokia 7x50 SR OS 20.10.R12).

Changes to TOE

For this Assurance Continuity, the version number of TOE changed from Nokia 7x50 SR OS 20.10.R4 to Nokia 7x50 SR OS 20.10.R12. The following paragraphs list the minor hardware and software changes made to the TOE during the maintenance cycle.

1. Hardware Changes

The developer reported the new hardware features/changes to the product located in the table below:

Support for MDA-e-XP 16pt 10/25G SFP28+2pt QSFP28 -B, MDA-s - 16pt SFPDD MACsec+4pt QSFP28 -B, and MDA-s - 8pt SFPDD MACsec+2pt QSFP28 -B

Release 20.10.R12 introduces the MDA-e-XP 16pt 10/25G SFP28+2pt QSFP28 -B on the 7750 SR product family. The MDA-s - 16pt SFPDD MACsec+4pt QSFP28 -B and MDA-s - 8pt SFPDD MACsec+2pt QSFP28 -B are introduced on the 7750 SR-s product family.

MACsec is not supported in Release 20.10.Rx for the MDA-s - 8pt SFPDD MACsec+2pt QSFP28 -B card.

- **Impact: Minor**
- **Rationale: This was an update to support additional pluggable cards in the chassis. These pluggable cards do not support MACsec and does not change the equivalency analysis. This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

QSFP28 100G LR Single Lambda

Release 20.10.R12 introduces support the for the QSFP28 100G LR single lambda pluggable module for the 7250 IXR, 7750 SR, 7750 SR-s, and 7950 XRS platforms.

- **Impact: Minor**
- **Rationale: This was an update to support additional pluggable cards in the chassis that does not change the equivalency analysis. This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

Support for QSFP28 100G ER4 0/70C

Release 20.10.R12 introduces support for the QSFP28 100G ER4 0/70C. This new pluggable is supported on the 7250 IXR, 7750 SR, 7750 SR-s, and 7950 XRS platforms.

- **Impact: Minor**
- **Rationale: This was an update to support additional pluggable cards in the chassis that does not change the equivalency analysis. This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

QSFP56-DD 4x100G LR

Release 20.10.R12 introduces support the for the QSFP56-DD 4x100G LR single lambda pluggable module for the 7250 IXR, 7750 SR, 7750 SR-s, and 7950 XRS platforms.

- **Impact: Minor**
- **This was an update to support additional pluggable cards in the chassis that does not change the equivalency analysis. This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

QSFP56-DD 400G ER8

Release 20.10.R12 introduces support the for the QSFP56-DD 400G ER8 pluggable module for the 7250 IXR, 7750 SR, 7750 SR-s, and 7950 XRS platforms.

- **Impact: Minor**
- **Rationale: This was an update to support additional pluggable cards to the hardware that does not change the equivalency analysis.**

QSFP-DD Support for 1x100g, 2x100g, and 3x100g

Release 20.10.R9 provides support of the 1x100g, 2x100g, 3x100g for the QSFP-DD 400G ZR+ optical modules.

- **Impact: Minor**
- **Rationale: This was an update to support additional connector breakout configurations to support various data speeds. This update does not change the equivalency analysis.**

Option to Configure DWDM Transmit Frequency

Release 20.10.R9 adds a new attribute to allow the configuration of the frequency of the transmit for a coherent DWDM port. This allows frequencies on grids other than the 100 GHz or 50 GHz grids to be specified for supported optical modules.

- **Impact: Minor**
- **Rationale: This was an update to the hardware that does not change the equivalency analysis.**

Support for QSFP28 100G ZR4 on the 7750 SR/SR-s

Release 20.10.R8 introduces support for the QSFP28 100G ZR4 on the 7750 SR/SRs for the following FP4-based hardware: XMA-s, 7750 SR-1s and the MDA-s for the 7750 SR-1s SR-1s Modular, SR-2s, SR-7s, SR-14s, and MDA-e-XP for the 7750 SR- 1, SR-7, SR-12, and SR-12e.

- **Impact: Minor**
- **Rationale: This was an update to support additional pluggable cards to the hardware that does not change the equivalency analysis.**

Support for QSFP28 BX20-U/D

Release 20.10.R8 introduces support for the QSFP28 100G BX20 (bidirectional) pluggable modules on the 7250 IXR-R6, IXR-6, IXR-10, IXR-X1, IXR-Xs, 7750 SR, and 7950 XRS platforms.

- **Impact: Minor**
- **Rationale: This was an update to support additional pluggable cards to the hardware that does not change the equivalency analysis.**

Support for SFP-DD 100G DR, FR, and LR Single Lambda Pluggable Modules

Release 20.10.R8 introduces support for the SFP-DD 100G DR, FR, and LR single lambda pluggable modules on the 7750 SR-s platform.

- **Impact: Minor**
- **Rationale: This was an update to support additional pluggable cards to the hardware that does not change the equivalency analysis.**

Support for QSFP-DD 400G ZR and ZR+ Optical Modules

Release 20.10.R7 introduces support for the QSFP-DD 400G ZR and QSFP-DD 400G ZR+ coherent pluggable modules.

- **Impact: Minor**

- **Rationale: This was an update to support additional pluggable cards to the hardware that does not change the equivalency analysis.**

LR4 Optical Module on the ESA 100G

Release 20.10 R7 introduces support for the LR4 Optics (3HE10550AA QSFP28-100G LR4 10KM LC) optical module on the ESA 100G.

- **Impact: Minor**
- **Rationale: This was an update to support additional pluggable cards to the hardware that does not change the equivalency analysis.**

Support for SFP28 Tunable Optical Module on the 7250 IXR, 7750 SR, and 7750 SR-s

Release 20.10.R6 introduces the SFP28 25G tunable DWDM optical module supporting 40 channels and 100 GHz spacing. The SFP28 25G tunable DWDM optical module is supported on the following cards and systems: 7250 IXR-Xs, 7250 IXR-R4/R6 MDA 6pt 10G + 4pt 25G, 7250 IXR-e, MDA-s 16-port SFP-DD MACsec + 4pt QSFP28, MDA-s 8-port SFP-DD MACsec + 2-port QSFP28, and the MDA-e 8- port 10/25GE SFP+/28.

- **Impact: Minor**
- **Rationale: This was an update to support additional pluggable cards to the hardware that does not change the equivalency analysis. This was an update to a non-evaluated feature (MACsec is only supported on SR-1e but it was excluded from the evaluation) that does not affect the evaluated functionality.**

2. Software Changes

The developer reported the new software features/changes to the product located in the table below:

BGP

Release 20.10.R12 is enhanced to treat a received BGP update message with an Atomic-Aggregate path attribute flag value of “0x00 0x80 0xc0” as treat-as-withdraw when **update-fault-tolerance** is enabled or as session-reset when **update-fault-tolerance** is disabled. This change is made to conform with RFC 7606 section 3, clause c. [408832].

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

Application Assurance

Changes to modern browsers and handsets have made the underlying mechanism of AA's HTTPS redirect feature outdated. This means that on more recent systems, the scope of eligible sites for HTTPS redirect has been severely narrowed. In Release 20.10.R12, an update to the AA redirect mechanism restores the previous scope of eligible sites for more recent systems. As before, websites that the client has previous knowledge of stricter security policies (like Google, Facebook, and others) cannot be redirected. [407320].

- **Impact: Minor**
- **Rationale: This was a feature enhancement that does not change the demonstrated TOE boundary or any evaluated functionality.**

BFD

Release 20.10.R12 changes the restriction that a Seamless BFD (S-BFD) reflector can only be configured on a router comprising only FP3 or newer IOMs or IMMs. The check that is performed when configuring config>bfd>seamlessbfd> reflector is changed so that an S-BFD reflector can only be configured if all the network and hybrid ports are on FP3+ cards, and none of the network or hybrid ports are on FP2-based cards. [415636].

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

OAM

In Release 20.10.R12, TWAMP Light Session-Reflector processes the Z-bit from the Error Estimate filed and received in the TWAMP Light test packet from the Session-Sender. The Session-Reflector uses the inbound Z-bit to choose the timestamp format to encode in the response packet, replying in-kind, marking the Z-bit to align with the timestamp format encoded in the Session-Sender TWAMP Light test packet. [417211].

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

Release 20.10.R11 introduces improvements to BGP error handling for errors detected in received update messages. Most of the error handling improvements only apply when the BGP **update-fault-tolerance** command is enabled. These improvements align SR OS with RFC 7606.

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

Application Assurance

Release 20.10.R11 provides more flexibility to operators using web filtering by introducing the “Marijuana” and “Provocative Attire” categories. Operators can configure these categories to allow, block, or redirect like the already supported categories. [403980].

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

IPsec/TLS

CVE-2022-0778 describes a vulnerability in OpenSSL where it is possible to trigger an infinite loop by crafting a certificate that has invalid elliptic curve parameters. Since certificate parsing happens before verification of the certificate signature, a process that parses an externally supplied certificate may be subject to a denial-of-service attack.

In Release 20.10.R10, this vulnerability was fixed.

- **Impact: Minor**
- **Rationale: This was a security fix to mitigate a vulnerability. This does not affect the evaluated functionality.**

Timing/Clocking

In Release 20.10.R9, as a grandmaster clock, PTP supports clock class 7 (in holdover, within holdover specification). During a short interruption of the local GNSS port, PTP degrades the clock class from 6 to 7, instead of 248. This allows better interoperability with some implementation of PTP slave clocks, which do not synchronize to a master clock advertising clock class 248. [403029].

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

System

Release 20.10.R6 introduces the following commands for the 7750 SR-s PSUs. [377870].

- A command to initiate operational off/operational on to reset the output power of a specified PSU in the chassis (**clear chassis power-shelf** *power-shelf-id* **power-module** *power-module-id*).
- A command to display PSU telemetry (**tools dump power-shelf** *power-shelf-id* **power-module** *power-module-id* **telemetry**).
- A command to clear latched faults that are no longer current (**tools perform power-shelf** *power-shelf-id* **power-module** *power-module-id* **clear-faults**).

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

BGP

Release 20.10.R6 enhances BGP so that when a received BGP route with an IGP cost to reach its BGP next hop of value M is imported into another BGP RIB and then re-advertised to other BGP peers subject to a **med-out igp-cost** command (or the policy equivalent), the MED correctly indicates a value of M rather than zero. [381301].

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

MD-CLI

The MD-CLI **bof auto-configure** and **bof auto-boot dhcp** commands are now ready for production networks. This feature was introduced in Release 20.10.R1.

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

gNMI

Release 20.10.R5 introduces the ability for the gNMI client to retrieve information about how PROTO encoding must be decoded. This information can be obtained by requesting the path with the “gnmi.schemas” origin. [370174]

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

Subscriber Management

Release 20.10.R5 introduces the **tools perform subscriber-mgmt systembehavior laa-priority** command to lower the authentication origin priority for **local-address-assignment client applications ppp-v4**. With this feature enabled, RADIUS can override DNSv4 server addresses obtained using LAA and assigned to PPPoE sessions. Contact your Nokia representative for more details.

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

Application Assurance

Release 20.10.R5 introduces AA transit-IP subscriber support on ESA 100G. [369135].

- **Impact: Minor**
- **Rationale: This was an update to a non-evaluated feature that does not affect the evaluated functionality.**

3. Changes to Evaluation Documents

The AGD document has been updated to identify the new TOE version and to an updated version of 0.8, May 30, 2023.

The Security Target document has been updated to identify the new TOE version and has been updated to version 3.1, May 30, 2023.

Regression Testing

In addition to the vendor performing vulnerability testing, functional regression testing, and unit testing is also performed against each release and/or software build to ensure the TOE functionality is maintained and that the source code is fit for use. This functional testing included verification that any newly introduced feature does not affect the security functionality previously tested and verified.

The regression testing performed against the TOE includes partial automation testing as well as manual test execution by the Quality Assurance Team within Nokia. This testing ensures that the functionality claimed within the Security Target has not been impacted by any software changes made to the product between releases.

The unit testing is performed against each software build to ensure that the source code used in each release is fit for use and performing in the expected manner.

For instances when security related bugs were identified, the vendor performed specific testing on the updates to ensure that the identified behavior is no longer present within the TOE and the TOE operates as expected. For example, when bugs related to memory leaks are incorporated into the TOE software, the vendor performs the operations that resulted in the memory leak to ensure that the operations no longer result in the memory leak. After this is successfully confirmed, the testing is incorporated into the regular regression testing and rerun until the TOE software is released.

NIST CAVP Certificates

No changes to the CAVP certificates from the previously evaluated version of the TOE.

Vulnerability Analysis

On October 3, 2023, the evaluator examined sources of publicly available information to identify potential vulnerabilities in the TOE. The sources of examined are as follows:

- https://nvd.nist.gov/vuln/search
- https://cve.mitre.org/
- https://www.tenable.com/cve
- http://www.zerodayinitiative.com/advisories
- https://www.rapid7.com/db/vulnerabilities
- https://www.nokia.com/networks/products/7750-service-router/ - Vendor Website

The evaluator examined public domain vulnerability searches by performing a keyword search. The terms used for this search were based on the vendor’s name, product name, and key platform features leveraged by the product. As a result, the evaluator performed a search using the following keywords:

- Nokia Service Router
- 7750 Service Router
- 7750 SR-1
- 7750 SR-1s
- 7750 SR- 2s
- 7750 SR-7s
- 7750 SR-14s
- 7950 XRS-20
- 7950 XRS-16c

- 7450 ESS
- 7750 SR-1e
- TLS v1.2
- SSH v2
- SRCM 3.1
- OpenSSL 1.1.1g
- TCP
- Nokia 7750 SR OS 20.10.R12

Vulnerability analysis included search of vulnerabilities applicable to the TOE and all the third-party software included as part of the TOE. The issues found were either for those where fixes have been applied in the updated TOE, or were related to other products, not applicable to the TOE in the evaluated configuration or justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP].

Conclusion

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. No functionality, as defined in the SFRs, was impacted, and none of the hardware and software updates affected the security functionality or the SFRs identified in the Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.