Australian Information Security Evaluation Program

Maintenance Report for

Juniper Junos OS 20.2R1 for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX380 and SRX1500

Version 1.0, 30 August 2023

Report Identifier: AISEP-CC-MR-2023-AAC091

Original (Certified) TOE

Juniper Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC and SRX1500

Table of contents

Introduction 3

Overview 3

Changes to Evaluation Documentation 3

Changes to the TOE 4

Hardware 4

Software 4

Guidance 4

Regression Testing 4

Vulnerability Search 5

Conclusion 5

References 6

Introduction

Overview

This document is an Assurance Continuity Maintenance Report describing the findings of the Australian Information Security Evaluation Program (AISEP) concerning the certification of Juniper Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380 and SRX1500.

The purpose of this Maintenance Report is to describe the status of the assurance continuity activities undertaken by Juniper against the requirements contained in *Assurance Continuity: CCRA Requirements v2.2, 2021-Sep-30* (Ref [1]).

On behalf of Juniper, Teron Labs submitted *Impact Analysis Report Juniper Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380 and SRX1500* to the Australian Certification Authority (ACA) on 15 August 2023. The Impact Analysis Report (IAR) describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes. The change involves the addition of three models into the scope of the original certification, the SRX300, SRX320 and SRX340.

The evaluation evidence submitted for consideration included a new Security Target (ST), new Common Criteria Guidance Documents, revised test documentation and an IAR.

Changes to Evaluation Documentation

The Certified TOE is Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380 and SRX1500. The Maintained TOE is Junos OS 20.2R1 for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX380 and SRX1500.

Certified TOE →	**Maintained TOE**
Security Target: Security Target for Junos OS 20.2R1 SRX345, SRX345-DUAL-AC, SRX380 and SRX1500 Version 1.4, Nov 02, 2020	Maintained Security Target: Security Target for Junos OS 20.2R1 for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX380 and SRX1500 Version 1.5 July 19, 2022
Common Criteria Guidance Documentation: Junos OS Common Criteria Guide for SRX345, and SRX380 Devices, Release 20.2R1, Date 2020-09-03 Junos OS Common Criteria Guide for SRX1500 Devices, Release 20.2R1, Date 2020-09-30	Maintained Common Criteria Guidance Documentation: Junos OS Common Criteria Guide for SRX300, SRX320, SRX340, SRX345, SRX345-Dual-AC, and SRX380 Devices, Release 20.2R1, Date 2022-07-19 Junos OS Common Criteria Guide for SRX1500 Devices, Release 20.2R1, Date 2022-07- 18
Certification Report: Certification Report Juniper Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380 and SRX1500, Version 1.0, 03 December 2020	Maintenance Report: Maintenance Report for Juniper Junos OS 20.2R1 for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX380 and SRX1500, Version 1.0, 30 August 2023

Vulnerability Analysis: Evaluation Workbook: AVA EFT-T013-EWB-AVA V1.0	Updated Vulnerability Analysis: Evaluation Workbook: AVA EFT-T013-EWB-AVA V1.1
Original Testing: Test Report NDcPP Junos 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380 and SRX1500 EFT-T013-TR-NDcPP 1.0 EFT-T013-TR-IPSEP 1.2 EFT-T013-TR-MOD_FWcPP 1.2 EFT-T013-TR-NDcPP 1.2	Extended Testing: Test Report NDcPP Junos 20.2R1 for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX380 and SRX1500 EFT-T013-TR-NDcPP 1.2 EFT-T013-TR-IPSEP 1.2 EFT-T013-TR-MOD_FWcPP 1.2 EFT-T013-TR-NDcPP 1.2

Changes to the TOE

Hardware

Three new hardware platforms have been added to the TOE, the SRX300, SRX320 and SRX340. The SRX340 uses the same processor as the SRX345 and SRX345-DUAL-AC. The SRX300 and SRX320 use a similar processor in the same Octeon III multi-core MIPS64 processor family that is used in the SRX340, SRX345, SRX345-DUAL-AC and SRX380.

Software

No changes have been made to the TOE software version.

Guidance

The Security Target and Common Criteria Guidance Documents were updated to include the new hardware platforms.

Regression Testing

Since the software for the maintained TOE was the same version as the certified TOE no regression testing was performed on the existing hardware platforms. Testing was performed on a suitable sample of the added hardware platforms by Teron Labs on behalf of Juniper. These testing results were provided to the ACA.

Vulnerability Search

A vulnerability search of public sources was carried out in June 2023 by Teron Labs on behalf of Juniper. The following terms were used in the search:

- "firewall"
- "router"
- "TCP"
- "UDP"
- "IPv4"
- "IPv6"
- "SSH"
- "IPsec"
- "Junos"
- "20.2R1"
- "Juniper SRX"
- "OpenSSL 1.0.2u"
- "FreeBSD 11"
- "SRX300"
- "SRX320"
- "SRX340"
- "SRX345"
- "SRX380"
- "SRX1500"

New potential vulnerabilities found were analysed. None were found to be exploitable considering an attacker possessing a basic attack potential.

Conclusion

After consideration of the Impact Analysis Report (IAR) provided by Teron Labs the Australian Certification Authority (ACA) has determined that the proposed changes are minor. The ACA agrees that the resultant change in the TOE can be classified as minor and that certificate maintenance is the correct path to continuity of assurance. The ACA agrees that the original assurance result is acceptable for the maintained TOE, Juniper Junos OS 20.2R1 for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, SRX380 and SRX1500.

References

1. *Assurance Continuity: CCRA Requirements, version 2.2, 2021-Sep-30*
2. National Information Assurance Partnership/Common Criteria Evaluation and Validation Scheme, Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, 12 September 2016, Version 3.0
3. *Impact Analysis Report, Juniper Junos OS 20.2R1 for SRX345, SRX345-DUAL-AC, SRX380 and SRX1500 Impact Analysis Report v1.0*
4. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
5. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
6. Protection Profiles:
    a) *collaborative Protection Profile for Network Devices, Version 2.1*
    b) *PP-Module for Stateful Traffic Filter Firewalls, Version 1.3*
    c) *PP-Module for Virtual Private Network (VPN) Gateways, version 1.0*
    d) *Extended Package for Intrusion Prevention Systems, version 2.11*
7. Guidance documentation:
    a) Junos Common Criteria Guide for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC, and SRX380 Devices, 2022-07-19
    b) Junos Common Criteria Guide for SRX1500 Devices, 2022-07-18