



**ASSURANCE MAINTENANCE REPORT MR2
(supplementing Certification Report No. CRP248
and Assurance Maintenance Report MR1)**

**Juniper Networks EX3200 and EX4200 Switches
running JUNOS 9.3R2**

Version 9.3R2

Issue 1.0

April 2011

© Crown Copyright 2011 – All Rights Reserved

Reproduction is authorised, provided
that this report is copied in its entirety.

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT (ADDENDUM)

The IT products detailed below have been certified under the terms of the UK IT Security Evaluation and Certification Scheme and have met the specified Common Criteria (CC) requirements. The scope of the certification and the assumed usage environment are specified in the body of this report.			
Sponsor:	Juniper Networks, Inc.	Developer:	Juniper Networks, Inc.
Products, Versions/Releases:	MR2 Derived: Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2 Original: Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1		
Platforms:	(See above)		
Description:	The Juniper platforms are designed as hardware devices, which perform all routing/switching functions internally to the device. All router/switch platforms are powered by the same JUNOS software, which provides management and control functions as well as all IP routing.		
CC Version:	Version 3.1		
CC Part 2:	Conformant	CC Part 3:	Conformant
EAL:	EAL3 augmented by ALC_FLR.3		
PP Conformance:	None		
Related CC Certificates:	P248 and P248 Maintenance Addendum 1		
Date Maintained:	8 April 2011		
<p>The evaluation and maintenance was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.</p> <p>The purpose of the evaluation and maintenance was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], [ST2], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated and maintained against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.</p> <p>The issue of an Assurance Maintenance Report and a Certificate Maintenance Addendum is a confirmation that the evaluation process has been performed properly and that no <i>exploitable</i> vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.</p>			




 122	<p>The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to EN 45011:1998 (ISO/IEC Guide 65:1996) to provide product conformity certification as follows:</p> <p>Category: Type Testing Product Certification of IT Products and Systems.</p> <p>Standards:</p> <ul style="list-style-type: none"> • Common Criteria for Information Technology Security Evaluation (CC) EAL1 - EAL7; and • Information Technology Security Evaluation Criteria (ITSEC) E1 - E6. <p>Details are provided on the UKAS website (www.ukas.org).</p>
	<p style="text-align: center;"><i>Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA), May 2000</i></p> <p>The CESG Certification Body is a Participant to the above Arrangement [CCRA]. The Participants to the Arrangement are detailed on the Common Criteria Portal (www.commoncriteriaportal.org). The mark (left) confirms that the Common Criteria certificate has been authorised by a Participant to the above Arrangement and it is the Participant's statement that the certificate has been issued in accordance with the terms of the above Arrangement. Upon receipt of the certificate, the vendor(s) may use the mark in conjunction with advertising, marketing and sales of the IT product for which the certificate is issued.</p>
	<p style="text-align: center;"><i>Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA), Version 3.0</i></p> <p>The CESG Certification Body is a Participant to the above Agreement [MRA]. The current Participants to the Agreement are Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The mark (left) confirms that the conformant certificate has been authorised by a Participant to the above Agreement and it is the Participant's statement that the certificate has been issued in accordance with the terms of the above Agreement. The judgments contained in the certificate and in this associated Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the mark does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.</p>

TABLE OF CONTENTS

CERTIFICATION STATEMENT (ADDENDUM)	2
TABLE OF CONTENTS	3
I. INTRODUCTION	4
Overview	4
Maintained Versions	4
Assurance Continuity Process	5
General Points	5
II. ASSURANCE MAINTENANCE	6
Analysis of Changes	6
Changes to Developer Evidence	6
TOE Identification	6
TOE Scope and TOE Configuration	7
TOE Documentation	7
TOE Environment	7
III. TOE TESTING	8
Vulnerability Analysis	8
TOE Testing	8
IV. SUMMARY, CONCLUSIONS AND DISCLAIMERS	9
Summary	9
Conclusions	9
Disclaimers	9
V. REFERENCES	11
VI. ABBREVIATIONS	14

I. INTRODUCTION

Overview

1. This Assurance Maintenance Report (MR¹) [MR2] states the outcome of the Common Criteria (CC) [CC] Assurance Continuity [AC] process for *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*, as summarised on page 2 ‘Certification Statement (Addendum)’ of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.
2. The baseline for this Assurance Continuity (also known as Assurance Maintenance) report was the original CC evaluation of *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1*. That version was certified to CC EAL3, augmented with ALC_FLR.3, in February 2009.
3. Prospective consumers are advised to read this document [MR2] in conjunction with the following documents (available on the CESG and CC websites):
 - a) the Security Target [ST] for the original certified Target of Evaluation (TOE), which specifies the functional, environmental and assurance requirements for the evaluation;
 - b) the Certification Report [CR] for the original certified TOE;
 - c) the updated Security Target [ST1] for the first maintained derivative;
 - d) the Assurance Maintenance Report [MR1] for the first maintained derivative;
 - e) the updated Security Target [ST2] for the second (i.e. latest) maintained derivative.
4. The Developer of the certified TOE, and the two derived maintained versions, is detailed on page 2 ‘Certification Statement (Addendum)’ of this report and elaborated further on the CESG website (www.cesg.gov.uk).

Maintained Versions

5. The version of the product originally evaluated was:
 - *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1*
6. The first derived version of the product for which assurance was maintained was:
 - *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*

¹ Note that Assurance Maintenance Report (AMR) is sometimes abbreviated to Maintenance Report (MR).

7. The second derived version of the product for which assurance is maintained is:
- *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*
8. The maintenance of the second derived version is described in this document [MR2], which provides a summary of the incremental changes from the previous certified version [CR] and the previous maintained version [MR1].

Assurance Continuity Process

9. The Common Criteria Recognition Arrangement (CCRA) [CCRA] has been established as a basis for the mutual recognition of the results of Common Criteria evaluations. The process of Assurance Continuity within the CC is defined in the document ‘Assurance Continuity: CCRA Requirements’ [AC] and UK specific aspects are presented in [UKSP03P2].

10. The Assurance Continuity process is based on an Impact Analysis Report (IAR) produced by the Developer. The IAR describes all the changes made to the product, together with the updated evaluation evidence, and assesses the security impact of each change. For *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*, the IAR [IAR2] has been examined by the CESG Certification Body (CB), who produced this Maintenance Report [MR2].

11. The Developer, Juniper Networks, Inc., has considered all the relevant assurance aspects detailed in ‘Assurance Continuity: CCRA Requirements’ [AC]. No retesting was required for *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2* because:

- a) There were no changes in the TOE software images since the first derived version [MR1].
- b) There were no changes to the TOE platforms listed in the security target [ST2] since the first derived version [ST1].

General Points

12. Assurance Continuity addresses the security functionality claimed in the updated Security Target [ST2] with reference to the assumed environment specified. The assurance-maintained TOE configurations and platform environments are as specified by the modifications detailed in Chapter II of this report [MR2], in conjunction with the original Certification Report [CR] and the previous Maintenance Report [MR1]. Prospective consumers are advised to check that this matches their identified requirements.

II. ASSURANCE MAINTENANCE

Analysis of Changes

13. [IAR1] provides the Impact Analysis Report from *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1* to *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*, and provides the Assurance Continuity rationale for the maintained TOE on the stated platforms. [IAR2] provides the Impact Analysis Report from the first derived version to the second derived version of *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*. [IAR2] conforms to the Assurance Continuity requirements specified in [AC], in particular Chapters 4 and 5.

14. No major changes were made between the certified version and the first derived version, and no major changes were made between the first derived version and the second derived version.

15. The updated Security Target [ST2] and updated Secure Configuration Guide [SCG2] for CC consumers have incorporated changes to remove references to the use of the management GUIs and to ensure that access to the GUIs is disabled in the CC evaluated configuration. There were no bug fixes, since the TOE software and platforms had not changed. There were no changes to the development environment and hence no changes that impacted the ALC_FLR.3 augmentation.

16. Consequently, only minor changes were required to [ST1] to obtain the Security Target for the second derived version [ST2].

Changes to Developer Evidence

17. [IAR2] and [IAR2S] show that the evaluation documentation deliverables that were updated for *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2* were as follows:

- a) Security Target [ST2]: updated from [ST1] which was previously updated from [ST].
- b) Secure Configuration Guide [SCG2]: updated from [SCG], which was applicable to both [ST] and [ST1].

18. The CESG CB agreed with the Sponsor/Developer that a Vulnerability Analysis was not required because the only change provided reduced interfaces through which to manage the evaluated configuration of the TOE.

19. All updates in the above documents were classified as *Minor*. There were no changes to any other evaluation documentation.

TOE Identification

20. The maintained TOE is uniquely identified as:

- **Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2**

TOE Scope and TOE Configuration

21. The TOE scope has been changed in Section 1.5 of [ST2], such that the management GUI is no longer in scope and access to the management GUI is disabled.
22. The TOE configuration is defined in [SCG2].

TOE Documentation

23. Apart from the Security Target [ST2] and the Secure Configuration Guide [SCG2], the TOE documentation has not changed.

TOE Environment

24. Apart from moving the management GUI from the TOE to the environment, the rest of the defined environment has not changed and is defined in [ST2].

III. TOE TESTING

Vulnerability Analysis

25. As the certified version [CR] and the first maintained version [MR1] were completed in the same timeframe, no further Vulnerability Analysis work was required at that time [IAR1]. For the second maintained version, covered by this report [MR2], the CESG CB agreed with the Sponsor/Developer that a Vulnerability Analysis was not required because there was only a *Minor* change to the evaluated configuration of the TOE [IAR2].

26. During the original evaluation, the Vulnerability Analysis was based on a search of public domain sources. As mentioned above, it was not necessary for that search to be repeated for the first and second maintained versions. As the scope of the TOE and the deliverables were unchanged, the mitigation of these vulnerabilities was unchanged from that reported in [ETR].

27. Chapter 5 of [IAR2] presents a justification that a search for vulnerabilities was not required.

28. Therefore, no vulnerabilities were found between the certified version of the TOE and the first and second maintained versions of the TOE.

TOE Testing

29. No functional or penetration testing was required for the second derived version of the TOE because there were no changes in the TOE software images and no changes in the TOE platforms since the first derived version. The *Minor* change to the evaluated configuration did not require any testing.

IV. SUMMARY, CONCLUSIONS AND DISCLAIMERS

Summary

30. The analyses in [IAR2] show that no major changes have been made to the TOE between the first and second derived versions of *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*. Thus all changes are categorised as having a *Minor* impact and hence CC EAL3 augmented with ALC_FLR.3 assurance has been maintained.

Conclusions

31. The CESG Certification Body accepts the decisions detailed in [IAR2] and [IAR2S]; and concludes that the overall impact of all the changes is *Minor*.

32. The CESG Certification Body has therefore determined that EAL3 augmented with ALC_FLR.3 assurance, as outlined in Certification Report CRP248 [CR] and the first Maintenance Report [MR1], has been maintained for the second derived version, *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*. Those conclusions are summarised in the ‘Certification Statement (Addendum)’ on Page 2 of this report.

33. Prospective consumers of *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2* should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST2]. The TOE should be used in accordance with the environmental assumptions specified in that Security Target. Prospective consumers are advised to check that the Security Functional Requirements (SFRs) and the evaluated configuration [SCG2] match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

34. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. A number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE are included in Certification Report CRP248 [CR].

Disclaimers

35. The Assurance Continuity process is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after the Assurance Continuity process has been completed. This Maintenance Report reflects the CESG Certification Body’s view at the time of certification.

36. Existing and prospective consumers should check regularly for themselves, in accordance with their Site Security Policy, whether any security vulnerabilities have been discovered since this Report was issued and, if appropriate, should check with the vendor to see if any patches exist for the product and whether those patches have further assurance.



37. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

38. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

V. REFERENCES

Common Criteria Documents

- [AC] Assurance Continuity: CCRA Requirements, Common Criteria Interpretation Management Board, CCIMB-2004-02-009, Version 1.0, February 2004.
- [CC] Common Criteria for Information Technology Security Evaluation, (comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).
- [CC1] Common Criteria for Information Technology Security Evaluation, Part 1, Introduction and General Model, Common Criteria Maintenance Board, CCMB-2006-09-001, Version 3.1 R1, September 2006.
- [CC2] Common Criteria for Information Technology Security Evaluation, Part 2, Security Functional Requirements, Common Criteria Maintenance Board, CCMB-2007-09-002, Version 3.1 R2, September 2007.
- [CC3] Common Criteria for Information Technology Security Evaluation, Part 3, Security Assurance Requirements, Common Criteria Maintenance Board, CCMB-2007-09-003, Version 3.1 R2, September 2007.
- [CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, Participants in the Arrangement Group, May 2000.
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, CCMB-2007-09-004, Version 3.1 R2, September 2007.
- [MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, Management Committee, Senior Officials Group – Information Systems Security (SOG-IS), Version 3.0, January 2010 (effective April 2010).

UK IT Security Evaluation and Certification Scheme Documents

- [UKSP00] Abbreviations and References, UK IT Security Evaluation and Certification Scheme, UKSP 00, Issue 1.6, December 2009.
- [UKSP01] UK Scheme Publication No. 1: Description of the Scheme, UK IT Security Evaluation and Certification Scheme, UKSP 01, Issue 6.3, December 2009.

- [UKSP02P1] UK Scheme Publication No. 2: CLEF Requirements, Part I – Start Up and Operation, UK IT Security Evaluation and Certification Scheme, UKSP 02: Part I, Issue 4.2, December 2009.
- [UKSP02P2] UK Scheme Publication No. 2: CLEF Requirements, Part II – Conduct of an Evaluation, UK IT Security Evaluation and Certification Scheme, UKSP 02: Part II, Issue 2.4, December 2009.
- [UKSP03P1] UK Scheme Publication No. 3: Sponsor’s Guide, Part I – General Introduction, UK IT Security Evaluation and Certification Scheme, UKSP 03: Part I, Issue 2.2, December 2009.
- [UKSP03P2] UK Scheme Publication No. 3: Sponsor’s Guide, Part II – Assurance Continuity, UK IT Security Evaluation and Certification Scheme, UKSP 03: Part II, Issue 1.0, December 2009.

Evaluated Version (Original)

- [CR] Certification Report No. CRP248, UK IT Security Evaluation and Certification Scheme, Issue 1.0, February 2009.
- [ETR] Evaluation Technical Report: Juniper Networks Services Routers running JUNOS 9.3R1, BT CLEF, LFS/T556/ETR, Issue 1.0, 15 January 2009.
- [SCG] Secure Configuration Guide for Common Criteria and JUNOS-FIPS, Juniper Networks, Inc., Release 9.3, January 2009.
- [ST] Security Target for Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1, Juniper Networks, Inc., Version 1.0, 13 January 2009.

First Derived Version

(Note that [SCG] was also applicable to the first derived version.)

- [IAR1] Impact Analysis Report JUNOS 9.3R2.8, Icon Security Ltd. for Juniper Networks, Inc., Version 1.1, 3 February 2009.

CRP248 MR2 – JUNOS 9.3R2

[MR1] Assurance Maintenance Report MR1
(supplementing Certification Report No. CRP248),
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, February 2009.

[ST1] Security Target for Juniper Networks EX3200 and EX4200 Switches
running JUNOS 9.3R2,
Juniper Networks, Inc.,
Version 1.0, 30 January 2009.

Second Derived Version

[IAR2] Impact Analysis Report JUNOS 8.5 & 9.3,
Icon Security Ltd. for Juniper Networks, Inc.,
Version 1.2, 5 April 2011.

[IAR2S] Review Form (Supplement to [IAR2]),
CESG Certification Body and Icon Security Ltd.,
CB/110209/ISL/AC, Issue 1.1, 11 April 2011.

[SCG2] Secure Configuration Guide for Common Criteria and JUNOS-FIPS, Release 9.3,
Juniper Networks, Inc.,
Revision 5, 31 March 2011.

[ST2] Security Target for Juniper Networks EX3200 and EX4200 Switches
running JUNOS 9.3R2,
Juniper Networks, Inc.,
Version 1.4, 05 April 2011.

[MR2] (*this document*)



VI. ABBREVIATIONS

This list contains only abbreviations that are specific to the TOE. It does not include well-known IT terms (such as GUI, HTML) or standard CC abbreviations (such as TOE, TSF; see CC Part 1 [CC1]) or Scheme abbreviations (such as CESG, CLEF; see [UKSP00]).

FIPS	Federal Information Processing Standard
JUNOS	Juniper Operating System