122-B

ASSURANCE MAINTENANCE REPORT MR1
(supplementing Certification Report No. CRP248)

Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2

Version 9.3R2

Issue 1.0

February 2009

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

CERTIFICATION STATEMENT (ADDENDUM)

The 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 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.
Product and Version	**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
Platform	(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 Part 2	Conformant to CC Version 3.1 Revision 2
CC Part 3	Conformant to CC Version 3.1 Revision 2
EAL	EAL3 Augmented by ALC_FLR.3
SoF	*Not Applicable*
PP Conformance	*None*
Related CC Certificates	CRP248
Date Maintained	3 February 2009

The evaluation and maintenance was carried out 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 a Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation and maintenance was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST1], 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.

The issue of a Certification Report and Addendum is a confirmation that the evaluation process has been carried out properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

**ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOG-IS MRA logo which appears below:

- confirms that the certificate has been issued under the authority of a party to an international Mutual Recognition Agreement (MRA) [MRA] designed to ensure that security evaluations are performed to high and consistent standards;
- indicates that it is the claim of the evaluating party that its evaluation and certification processes meet all the conditions of the MRA.

The judgements[1] contained in the certificate, Certification Report and in this Maintenance Report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the logo of this Agreement does not imply acceptance by other Members of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

CCRA logo **CC logo** **SOG-IS MRA logo**

[1] All judgements contained in this Certification Report, excluding ALC_FLR.3, are covered by the CCRA [CCRA] and the MRA [MRA].

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 7
TOE Identification 7
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 10

Summary 10
Conclusions 10
Disclaimers 10

V. REFERENCES 12

VI. ABBREVIATIONS 14

I. INTRODUCTION

Overview

1. This Maintenance Report (MR) states the outcome of the Common Criteria (CC) [CC] Assurance Continuity 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 Common Criteria 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. See [ST], [ETR] and [CR] for full details.

3. Prospective consumers are advised to read this document [MR1] in conjunction with the following documents (available on the CESG and CC websites):

- the Certification Report CRP248 [CR] for the EAL3 evaluation of the original certified Target of Evaluation (TOE), to which this report is an Addendum;

- the Security Target [ST] of the certified TOE, which specifies the functional, environmental and assurance requirements for the evaluation;

- the updated Security Target [ST1] of the latest maintained derivative.

Maintained Versions

4. 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*

5. A subsequent derived version (which is also the latest derived version) of the product for which assurance was maintained is:

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

6. The maintenance of the latest derived version is described in this document [MR1], which provides a summary of the incremental changes from the previous certified version [CR].

7. The Developer of the Certified TOE and the derived version is detailed on page 2 'Certification Statement (Addendum)' of this report and elaborated further on the CESG website.

Assurance Continuity Process

8. 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 Common Criteria is defined in the document 'Assurance Continuity: CCRA Requirements' [AC].

9. 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*, [IAR1] has been examined by the CESG Certification Body, who produced this Maintenance Report No.MR1 [MR1].

10. The Developer, Juniper Networks, Inc., has carried out full retesting on *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*, and has considered all the assurance aspects detailed in 'Assurance Continuity: CCRA Requirements' [AC].

General Points

11. Assurance Continuity addresses the security functionality claimed in the Security Target [ST1] with reference to the assumed environment specified. The assurance maintained TOE configurations and platform environments are as specified by the modifications detailed in this [MR1] Report (see 'TOE Identification' and 'TOE Environment') in conjunction with the original Certification Report [CR]. Prospective consumers are advised to check that this matches their identified requirements.

II. ASSURANCE MAINTENANCE

Analysis of Changes

12. [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. [IAR1] conforms to the Assurance Continuity requirements specified in [AC], in particular Chapters 4 and 5.

13. No major changes were made between *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1* and *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*. All changes were bug fixes as described in [IAR1]. No changes were made to the development environment and there were no changes that impacted the ALC_FLR.3 augmentation, as there were no changes to any of the deliverables that provided input into the associated evaluation activity.

14. The TOE changes and their impact and effect on the evaluation deliverables are described in [IAR1], which shows that *for all changes*:

- the “Impact of Change” is determined to be “None” or “Minor”;
- the “Effect on evaluation deliverables” is determined to be “None”;
- the “Action” required for resolution is determined to be “None”.

15. Note that:

- Only minor generic changes were required to the Security Target [ST], to reflect TOE version changes, resulting in [ST1].

- Some of the changes were for platforms that were in the original certified evaluation *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1,* but are not included in the scope of the Assurance Continuity for *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*.

- Some of the changes related to product functionality which was not in the scope of the original evaluation, so was outside the scope of the Assurance Continuity for *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*.

- Some of the changes were related to availability or performance issues of the product, which were not related to any Security Functional Requirements (SFRs), and hence were considered to be out of scope.

- Some of the changes were not in scope of the EAL3 requirements. For example, changes to detailed design or implementation aspects of the product are not provided in the EAL3 deliverables. The evaluators relied on the re-testing to confirm that the TOE behaved in the same manner.

Changes to Developer Evidence

16. [IAR1] shows that the *only* evaluation documentation deliverables that were updated for *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2* were:

- Security Target [ST1], updated from [ST].
- Developer Tests, updated as a result of re-run and regression testing.
- Vulnerability Analysis, updated in [IAR1] Section 5[2].
- Configuration List, provided by [IAR1] Section 1.2 and Section 3.

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

TOE Identification

18. The maintained TOE is uniquely identified as:

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

TOE Scope and TOE Configuration

19. The TOE scope is unchanged and is described in Section 1.5 of [ST1].

20. The TOE configuration is defined in [SCG], which covers *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1* and also *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*.

TOE Documentation

21. The Installation, Configuration and Guidance documents are unchanged. [IAR1] provides the changes to the Configuration List, as noted in Paragraph 16 above.

TOE Environment

22. The defined environment has not changed and is defined in [ST1].

[2] Note that the Vulnerability Analysis in [IAR1] determined that no further work was required since the certified version [CR] and the maintained version [MR1] had been completed in the same timeframe.

III. TOE TESTING

Vulnerability Analysis

23. In order to assess whether any vulnerabilities had been introduced into the product between *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1* and *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*, an analysis was intended to be made of the Developer's Flaw Reporting Database and public domain vulnerabilities. However, [IAR1] determined that no further Vulnerability Analysis work was required since the certified version [CR] and the maintained version [MR1] had been completed in the same timeframe.

24. [IAR1] shows that there had been no flaws or bugs logged that required changes within the scope of the maintained TOE, between the certified version and the maintained version.

25. 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 maintained version. As the scope of the TOE and the deliverables were unchanged, the mitigation of these vulnerabilities was unchanged from that reported in [ETR].

26. Chapter 5 of [IAR1] presents a justification that a search for vulnerabilities was not required.

27. Therefore, no vulnerabilities were found between the certified version of the TOE and the currently maintained version of the TOE.

TOE Testing

28. The developer testing performed for the 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* was completely automated and was controlled by a set of test scripts. The developer testing was performed by Juniper Networks, Inc. The evaluator testing was based on functional and penetration test scripts.

29. The developer's automated test scripts examined during the original evaluation have been appropriately updated. However the actual tests themselves have not significantly changed and they test exactly the same security functionality in the same manner.

30. All test scripts used for testing *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2* were run on all platforms included within the scope of the maintenance and all of those tests passed. The results were exactly the same as the results of the tests performed during the original evaluation and did not reveal any inconsistencies or concerns.

31. Thus confidence can be gained that *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2* provides the claimed security functionality in the same manner as *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1*.

IV. SUMMARY, CONCLUSIONS AND DISCLAIMERS

Summary

32. The analyses in [IAR1] show that no major changes have been made to the TOE between *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1* and *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*. The only changes have been bug-fixes and these have all resulted in changes to the low level design or source code, and are at too low a level of detail to require any changes to the evaluation documentation produced at CC EAL3. Thus all changes are categorised as having a ***Minor*** impact and hence CC EAL3 augmented with *ALC_FLR.3* assurance has been maintained.

Conclusions

33. The Certification Body accepts the decisions detailed in [IAR1], which has assessed each change as being of ***Minor*** impact, and concludes that the overall impact of all the changes is ***Minor***.

34. The Certification Body has therefore determined that EAL3 augmented with *ALC_FLR.3* assurance, as outlined in Certification Report P248 [CR], has been maintained for the latest derived version, *Juniper Networks EX3200 and EX4200 Switches running JUNOS 9.3R2*. These conclusions are summarised in the 'Certification Statement (Addendum)' on Page 2.

35. 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 [ST1]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

36. 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 P248 [CR].

Disclaimers

37. 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 Certification Body's view at the time of certification.

38. 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.

39. 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.

40. 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

[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.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2007-09-004, 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.

[AC] Assurance Continuity: CCRA Requirements,
Common Criteria Interpretation Management Board,
CCIMB-2004-02-009, Version 1.0, February 2004.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee of Agreement Group,
Senior Officials Group – Information Systems Security,
Version 2.0, April 1999.

UK IT Security Evaluation and Certification Scheme Documents

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.5, October 2008.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.2, October 2008.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.1, October 2008.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.3, October 2008.

Evaluated Version (Original)

[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.

[SCG] Security Configuration Guide for Common Criteria and JUNOS-FIPS,
Juniper Networks, Inc.,
Release 9.3, January 2009.

[ETR] Evaluation Technical Report: Juniper Networks Services Routers running JUNOS 9.3R1,
BT CLEF,
LFS/T556/ETR, Issue 1.0, 15 January 2009.

[CR] Certification Report No. CRP248,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, February 2009.

First Derived Version

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

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

[MR1] *(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