CESG CERTIFICATION BODY

122-B

COMMON CRITERIA MAINTENANCE REPORT MR2 (supplementing Certification Report No. P237)

Juniper Networks J2300, J2350, J4300, M7i and M10i Services Routers running JUNOS 8.5R3

Issue 1.0

10 September 2008

Certification Body
CESG, Hubble Road
Cheltenham GL51 0EX
United Kingdom

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

The CESG Certification Body is a member of the above Arrangement and as such this confirms that the addendum to the original 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 addendum has been issued in accordance with the terms of this Arrangement.

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

The *IT Security Certified* logo which appears above:

- confirms that this certificate has been issued under the authority of a party to an international Recognition Agreement ('RA') 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 RA.

The judgements[1] contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out 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 upon those judgements by a third party.

The evaluation 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 was to provide assurance about the effectiveness of the TOE in meeting its Security Target [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 against this baseline. Both parts of the evaluation were performed in accordance[1] with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report 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.

Trademarks:

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

[1] All judgements contained in this Certification Report (i.e. Maintenance Report) are covered by the Recognition Arrangement.

Table of Contents

Abbreviations

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CLI	Command Line Interface
DNS	Domain Name Service
EAL	Evaluation Assurance Level
IAR	Impact Analysis Report
MR	Maintenance Report
SFR	Security Functional Requirement
TOE	Target of Evaluation

For completeness, please also refer to Chapter 3 *Terms And Definitions* and Chapter 4 *Symbols And Abbreviated Terms* in Part 1 of the Common Criteria [CC].

References

[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-2005-08-001, Version 2.3, August 2005.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-002, Version 2.3, August 2005.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-003, Version 2.3, August 2005.

[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-2005-08-004, Version 2.3, August 2005.

[CL2] Common Criteria Configuration List for JUNOS 8.5R3,
Juniper Networks, Incorporated,
Issue 1.0, August 2008.

[CR] Common Criteria Certification Report No. CRP237,
Juniper Networks M/T/J Series of Service Routers running JUNOS 8.1R1,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, April 2007.

[ETR] Juniper Networks M/T/J Series Families of Service Routers running JUNOS 8.1R1,
Evaluation Technical Report,
BT CLEF,
LFS/T532/ETR, Issue 1.0, 20 April 2007.

[IAR1] Juniper Networks M/T/J Series Families of Service Routers running JUNOS 8.1R3,
Impact Analysis Report,
BT CLEF,
LFS/T538, Version 1.0, December 2007.

[IAR2] Impact Analysis Report JUNOS 8.5R3.4,
Juniper Networks, Incorporated,
Version 2, 12 August 2008.

[MR1] Common Criteria Maintenance Report MR1
(supplementing Certification Report No. P237),
CESG Certification Body,
Issue 1.0, 11 February 2008.

[MR2] *(this document)*

[SCG2] Secure Configuration Guide for Common Criteria and JUNOS-FIPS,
Release 8.5,
Juniper Networks, Incorporated,
Part Number: 530-021951-01 , Revision 1.

[ST] Security Target for Juniper Networks M/T/J Series Families of Service Routers running JUNOS 8.1R1,
Juniper Networks, Incorporated,
Version 1.0, April 2007.

[ST1] Security Target for Juniper Networks J2300, J4350, J6350, M7i and M10i Service Routers running JUNOS 8.1R3,
Juniper Networks, Incorporated,
Version 1.0, January 2008.

[ST2] Security Target for Juniper Networks J2300, J2350, J4300, M7i and M10i Services Routers running JUNOS 8.5R3,
Juniper Networks, Incorporated,
Version 1.0, August 2008.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.1, March 2006.

[VUL] Juniper Networks M/T/J Series Families of Service Routers running JUNOS8.1R1,
Vulnerability Analysis,
Juniper Networks, Incorporated,
Revision 0.4, February 2007.

Introduction

1. This Maintenance Report outlines the current status of the Common Criteria (CC) [CC] Assurance Continuity process for *Juniper Networks J2300, J2350, J4300, M7i and M10i Services Routers running JUNOS 8.5R3*, 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 Assurance Continuity (also known as Assurance Maintenance) was the Common Criteria evaluation, to the EAL3 Evaluation Assurance Level, of *Juniper Networks M/T/J Series of Service Routers running JUNOS 8.1R1*.

3. Prospective consumers are advised to read this document [MR2] in conjunction with:

- the Certification Report P237 [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] and the Maintenance Report [MR1] of the first maintained derivative;
- the updated Security Target [ST2] of the second maintained derivative.

Maintained Versions

4. The version of the product originally evaluated was:

- *Juniper Networks M/T/J Series of Service Routers running JUNOS 8.1R1*.

5. The first derived version of the product for which assurance was subsequently maintained was:

- *Juniper Networks J2300, J4350, J6350, M7i and M10i Service Routers running JUNOS 8.1R3*.

6. The maintenance of the first derived version is described in [MR1], which provides a summary of the changes from the original product.

7. The second derived version of the product for which assurance has subsequently been maintained is:

- *Juniper Networks J2300, J2350, J4300, M7i and M10i Services Routers running JUNOS 8.5R3*.

8. The maintenance of the second derived version is described in this document [MR2], which provides a summary of the changes from the first derived version.

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

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 J2300, J2350, J4300, M7i and M10i Services Routers running JUNOS 8.5R3*, [IAR2] has been examined by the CESG Certification Body, who produced this Maintenance Report (MR) No. 2 [MR2].

11. The Developer, Juniper Networks, Incorporated, has carried out full retesting on *Juniper Networks J2300, J2350, J4300, M7i and M10i Services Routers running JUNOS 8.5R3*, and has considered all the assurance aspects detailed in 'Assurance Continuity: CCRA Requirements' [AC].

General Points

12. Assurance Continuity addresses the security functionality claimed in the 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 this MR2 Report (see ‘TOE Identification’ and ‘TOE Environment’) in conjunction with the original Certification Report [CR] and the first Maintenance Report [MR1]. Prospective consumers are advised to check that this matches their identified requirements.

13. 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 Report reflects the Certification Body’s view at the time of certification.

14. Existing and prospective consumers should check regularly for themselves 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.

15. 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 by a Scheme-approved Assurance Continuity process.

Analysis of Changes

16. JUNOS 8.1R1 was certified to the CC EAL3 level of assurance, augmented with ALC_FLR.3, in April 2007. See [ST], [ETR], and [CR] for full details.

17. [IAR1] provides the Impact Analysis Report from JUNOS 8.1R1 to JUNOS 8.1R3, and provides the Assurance Continuity rationale for JUNOS 8.1R3 on the following subset of platforms: J2300, J4350, J6350, M7i and M10i.

18. [IAR2] provides the Impact Analysis Report from JUNOS 8.1R3 to JUNOS 8.5R3 and provides the Assurance Continuity rationale for JUNOS 8.5R3 on the following subset of platforms: J2300, J2350, J4300, M7i and M10i. [IAR2] conforms to the Assurance Continuity requirements specified in [AC], in particular Chapters 4 and 5.

19. The Developer of the Certified TOE (JUNOS 8.1R1) and the Maintained TOEs (JUNOS 8.1R3 and JUNOS 8.5R3) is:

Juniper Networks, Incorporated
1194 North Mathilda Avenue
Sunnyvale
California 94089
USA

20. No major changes were made between JUNOS 8.1R3 and JUNOS 8.5R3. All changes were bug fixes as described in [IAR2]. No changes were made to the development environment and there were no changes that impacted the ALC_FLR.3 augmentation since there were no changes to any of the deliverables that provided input into the ALC_FLR.3 evaluation activity. The TOE changes and their impact and effect on the evaluation deliverables are described in [IAR2], which shows that *for all changes*:

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

21. Note that:

- Some of the changes were for platforms that were in the original JUNOS 8.1R1 evaluation but are not included in the scope of the Assurance Continuity for JUNOS 8.5R3: J2300, J2350, J4300, M7i and M10i.
- Some of the changes were related to the Command Line Interface (CLI) which was not included within the scope of the original evaluation and hence was considered to be outside the scope of the Assurance Continuity for JUNOS 8.5R3.

- Some of the changes were related to availability or performance of the TOE in general, which do not correspond to any Security Functions (and have no relation 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. However, the evaluators relied on the re-testing to confirm that the TOE behaved in the same manner.

- Some of the changes were not related to any Security Functions (and hence had no relation to any SFRs).

Changes to Developer Evidence

22. Note that [IAR2] shows that the *only* evaluation documentation deliverables that were updated were as follows:

- Results of Developer tests re-run on J2300, J2350, J4300, M7i and M10i platforms.

- Vulnerability Analysis (originally in [VUL]) updated in Chapter 5 of [IAR2].

- Secure Configuration Guide for Common Criteria and JUNOS-FIPS [SCG2], in order to reference JUNOS 8.5R3.

- JUNOS 8.5R3 Common Criteria Configuration List [CL2], in order to reference JUNOS 8.5R3.

- Security Target for Juniper Networks J2300, J2350, J4300, M7i and M10i Services Routers running JUNOS 8.5R3 [ST2], updated from [ST1] in order to reference JUNOS 8.5R3.

23. All updates in the above documents were classified as Minor.

TOE Identification

24. The maintained TOE is uniquely identified as:

- *Juniper Networks J2300, J2350, J4300, M7i and M10i Services Routers running JUNOS 8.5R3*

TOE Documentation

25. The TOE documents have changed as previously described in Paragraph 22.

TOE Environment

26. The defined environment has not changed.

Vulnerability Assessment

27. In order to assess whether any vulnerabilities had been introduced into the product between JUNOS 8.1R1 and JUNOS 8.1R3, an analysis was made of the Juniper Networks Flaw Reporting Database and public domain vulnerabilities. The same level of vulnerability analysis was performed for that re-assessment as was performed for the original evaluation. The information assessed also contained details of generic vulnerabilities, so any generic vulnerabilities relevant to JUNOS were also considered.

28. An analysis of the Juniper Networks Flaw Reporting Database was performed in November 2007. That showed that there had been no bugs logged that required changes within the scope of the maintained TOE between versions 8.1R1 and 8.1R3.

29. During the original evaluation a search of www.securityfocus.com and cve.mitre.org was performed on 19th February 2007 for vulnerabilities relating to JUNOS. That search was repeated on 21st November 2007 and it was found that no new vulnerabilities had been reported. As the scope of the TOE and the deliverables were unchanged, the mitigation of these vulnerabilities was unchanged from that reported in [ETR].

30. Chapter 5 of [IAR2] presents a summary of the search for vulnerabilities performed on the following websites in order to assess whether any vulnerabilities had been introduced into the product between JUNOS 8.1R3 and JUNOS 8.5R3:

- www.securityfocus.com
- cve.mitre.org
- www.cpni.gov.uk
- nvd.nist.gov
- www.kb.cert.org
- www.securitytracker.com
- www.securiteam.com
- www.securityreason.com.

31. In addition, [IAR2] noted a Domain Name Service (DNS) vulnerability, identified from the Juniper Knowledge Base, and determined that it was not applicable because the TOE does not include DNS services.

32. Therefore, no vulnerabilities were found between the previously maintained version of the TOE (JUNOS 8.1R3) and the currently maintained version of the TOE (JUNOS 8.5R3).

IT Product Testing

33. The testing performed for the evaluation of JUNOS 8.1R1 was completely automated and was controlled by a set of test scripts. The testing performed for JUNOS 8.5R3 was performed by the Regression Testing department at Juniper Networks, Incorporated.

34. The automated test scripts examined during the original evaluation and during the maintenance of JUNOS 8.1R3 were compared to the test scripts for JUNOS 8.5R3. Some of the test scripts have been renamed or split over two files. However the actual tests themselves have not changed and they test exactly the same functionality in the same manner.

35. All test scripts used for testing JUNOS 8.5R3 were performed on all five models included within the reassessment (J2300, J2350, J4300, M7i and M10i) 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.

36. Thus confidence can be gained that JUNOS 8.5R3 provides the claimed security functionality in the same manner as JUNOS 8.1R1 and JUNOS 8.1R3.

Summary

37. The analyses in [IAR2] show that no major changes have been made to the TOE between JUNOS 8.1R3 and JUNOS 8.5R3. The only changes have been bug-fixes and these have all resulted in changes to the code that are at too low a level of detail to require any changes to the design 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.

Conclusion

38. The Certification Body accepts the decisions detailed in [IAR2], which has assessed each change as being of ***Minor*** impact, and concludes that the overall impact of all the changes is ***Minor***. The Certification Body also accepts that [IAR2] meets the requirements for an Impact Analysis Report as specified in ‘Assurance Continuity: CCRA Requirements’ [AC].

39. After consideration of the [IAR2] and other visibility of the Assurance Continuity process given to the Certifier, the Certification Body has determined that EAL3 augmented with ALC_FLR.3 assurance, as outlined in Certification Report P237 [CR], has been maintained for the latest derived version, *Juniper Networks J2300, J2350, J4300, M7i and M10i Services Routers running JUNOS 8.5R3*. Only minor generic changes were required to the original Security Target [ST], to reflect TOE version changes, resulting in [ST2].