JANUARY 2013

Juniper JunOS 10.4R4

Product Description

1. Juniper's JunOS 10.4R4 is a software product that runs on proprietary Juniper hardware. A component of this software is the implementation of the Internet Protocol Security (IPsec) suite of protocols. This allows administrators to create a Virtual Private Network (VPN) between trusted networks over an untrusted network such as the Internet.

Evaluation Scope

2. The scope of the DSD Cryptographic Evaluation (DCE) included the following functionality:

   a. Correct implementation of the IPsec protocol

   b. Secure encryption key generation

   c. Secure certificate generation

Common Criteria Certification - Summary

3. The product was found to meet the requirements of the Common Criteria (CC) evaluation assurance level EAL4.

DSD Findings and Recommendations

4. DSD performed a cryptographic evaluation on the product in addition to the Common Criteria evaluation.

5. As the product has successfully completed a DCE, it can be used to communicate PROTECTED information over public network infrastructure in accordance with the Cryptography section of the Information Security Manual (ISM).

6. Agencies must configure the product to conform to the Internet Protocol Security controls in the ISM. However, the available HMAC algorithms (MD5-96-HMAC and SHA1-96-HMAC) are no longer in the list of DSD Approved Cryptographic Algorithms (DACAs). Agencies should refer to the guidance on DSD's website, www.dsd.gov.au/publications/csocprotect/sha-1_deprecated.htm, to understand the risks associated with the use of these superseded algorithms.

7. Agencies should disable remote management on the external interface. Management tasks should be performed from the internal network or over the VPN.

8. Agencies using remote management from the internal network should perform this function over a Secure Shell (SSH) channel configured to conform to the Secure Shell section of the ISM.

9. Agencies should disable unused functionality such as telnet and SSH. If these (or other) functions are required on the internal interface, they should still be disabled on the external interface.

10. Recommendations given in this consumer guide take precedence over those in the ISM where there is a conflict.

Contact

For further information regarding the certification, cryptographic evaluation or compliance with the ISM please contact DSD on 1300 CYBER1 (1300 292 371) or email dsd.assist@defence.gov.au.

ISM

The advice given in this document is in accordance with the ISM. Australian government agencies are reminded to periodically check the latest release date of the ISM at http://www.dsd.gov.au/infosec/ism/index.htm

Consumer Guide

This Consumer Guide was issued on 30 January 2013 by DSD