NOVEMBER 2015

# Juniper Junos 12.1X46-D37

## Product Description

1. Juniper Junos 12.1X46-D37 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 ASD Cryptographic Evaluation (ACE) included the following functionality:
   a. Correct implementation of the IPsec protocol
   b. Secure key generation
   c. Secure certificate generation

## Common Criteria Certification - Summary

3. A previous version (12.1X46-D20.6) of the product was found to meet the requirements of the Common Criteria (CC) Network Device Protection Profile (NDPP) v1.1 with the Firewall Extended Package (FWEP) v1.0 and Virtual Private Network Extended Package (VPNEP) v1.1.

4. The ACE was completed on Junos 12.1X46-D37, and ASD's recommendations apply to this version.

## ASD Findings and Recommendations

5. ASD performed a cryptographic evaluation on the product in addition to the Common Criteria evaluation.

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

7. Agencies must configure the product to conform to the Internet Protocol Security controls in the ISM.

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

9. 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.

10. 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.

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

## Contact Details

Australian government customers with questions regarding this advice should contact ASD Advice and Assistance at asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).