Cisco IOS/IPSec 12.3(6a)

Product Description

1. Cisco's Internetwork Operating System (IOS) is a software product that runs on proprietary Cisco hardware. A component of this software is the implementation of the IPSec suite of protocols. This allows system administrators to create a Virtual Private Network between trusted networks over an untrusted network such as the Internet.

Common Criteria Certification - scope

2. The scope of the Common Criteria (CC) evaluation included the following functionality:
   - IPSec implementation including IKE and ESP.
   - Key management in support of the IPSec implementation.
   - Packet filtering in support of the IPSec implementation.
   - Configuration and management of the IPSec function, primarily via an interactive CLI. Event logging facilities with reliable timestamps are also provided.

Common Criteria Certification – summary

3. The product has met the requirements of the Common Criteria evaluation assurance level EAL4. However, during the final stages of the evaluation the product was withdrawn from sale by Cisco due to issues found in the supporting IOS software environment that were outside the scope of the CC EAL4 evaluation.

4. Due to the issues with IOS/IPSec 12.3(6a) that led to its withdrawal from sale, DSD recommends that Australian Government agencies consider the use of a later version that does not suffer from these issues.

5. Cisco's IOS/IPSec 12.3(6f) has met the requirements for AISEP Certificate Continuity at the EAL4 level and is currently progressing with a DSD Cryptographic Evaluation. For more information see:

   www.dsd.gov.au/infosec/evaluation_services/epl/network_security/Cisco_IOSIPSec12.3.6f.html

DSD's Cryptographic Verification

6. As an adjunct to the Common Criteria evaluation, DSD verified, using information from earlier versions provided to DSD by Cisco, the implementation of a subset of the IPSec functions available in the 12.3(6a) version of the Cisco IOS. As part of this procedure the correct implementation of the authentication, encryption, IKE/ISAKMP and manual keying features was confirmed in software and hardware for the Tunnel Mode of operation using ESP.

7. The authentication features verified were:

   - the SHA-1 hashing algorithm,
   - the MD5 hashing algorithm,
   - correct handling of small and large data packets,
   - rejection of short authentication keys, and
   - truncation of long authentication keys.

8. The encryption features verified were:

   - 3DES encryption of data packets,
   - correct encryption of small and large data packets,
   - rejection of short encryption keys, and
   - truncation of long encryption keys.

9. The IKE/ISAKMP features verified were:

   - pre-shared keys, and
   - RSA encrypted nonces.

10. Note: the features that were excluded from the verification of IPSec in the 12.3(6a) version of the Cisco IOS were:

    - the Transport Mode of operation using AH or ESP,
    - the Tunnel Mode of operation using AH,
    - IKE/ISAKMP using RSA signatures.

DSD findings - summary

11. As a result of the cryptographic verification process undertaken, it was found that the software engine for each router was correctly implemented for SHA-1 and MD5 authentication, 3DES encryption, manual keying and IKE/ISAKMP using pre-shared keys and RSA encrypted nonces. Using the hardware cryptographic engines supplied for each router it was found that all routers were incapable of operating correctly when manually keyed and the successful operation of RSA encrypted nonces depended on the particular hardware engine being used.

DSD's Recommendations

12. For Australian Government users the following cryptographic configuration is recommended:

    - Tunnel Mode of operation using ESP;
    - 3DES as per DSD Approved Cryptographic Algorithm that meets ACSI 33;
    - if using IKE/ISAKMP, utilising Main Mode of operation;
    - SHA-1 or MD5 as hashing algorithms that meets ACSI 33;
    - key generation using modulus sizes of 1024 bits or larger as per ACSI 33;
    - a Diffie-Hellman Group with modulus size of 1024 bits or larger as per ACSI 33; and
    - a maximum Security Association lifetime of 4 hours (14400 seconds).

13. The product has been evaluated to EAL 4. In accordance with ACSI 33 Chapter 9, it can therefore be used for the transit of encrypted information of classification

    - IN-CONFIDENCE over an UNCLASSIFIED network;
    - RESTRICTED over UNCLASSIFIED, PROTECTED or HIGHLY PROTECTED networks;
    - PROTECTED over UNCLASSIFIED or IN-CONFIDENCE networks; and
    - HIGHLY PROTECTED over UNCLASSIFIED, IN-CONFIDENCE or PROTECTED networks.

Contact

14. For further information regarding Cisco's IOS/IPSec 12.3(6a) certification or compliance with ACSI 33 please contact DSD on (02) 6265 0197 or email assist@dsd.gov.au.

ACSI 33

10. The advice given in this document is in accordance with ACSI 33 release date September 2006. Australian Government agencies are reminded to check the latest release of ACSI 33 at

    www.dsd.gov.au/library/infosec/acsi33.html to investigate if any changes have taken place.

Consumer Guide - date

11. This Consumer Guide was issued on 22 December 2006, by DSD.