PROTECT

UPDATED: JUNE 2016
PUBLISHED: AUGUST 2013

Fortinet FortiOS 4.0 MR3

Product Description

1. Fortinet FortiOS 4.0 MR3 is a network operating system that runs on Fortinet routers and switches. Among other functions it can be used to establish Internet Protocol Security (IPSec) Virtual Private Network (VPN) tunnels. Fortinet's FortiGate Next Generation Security appliance is a proprietary hardware solution providing network security functionality. A component of this solution is the implementation of the 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) of Fortinet FortiOS 4.0 MR3 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. Fortinet FortiGate Unified Threat Management Solutions and FortiOS 4.0 CC Compliant Firmware FortiOS 4.0 MR3 were evaluated and certified to Evaluation Assurance Level (EAL) 4+ by the Canadian Common Criteria Evaluation and Certification Scheme (CCS) on 11 March 2013.

ASD Findings and Recommendations

4. ASD performed a cryptographic evaluation on Fortinet FortiOS 4.0 MR3 in addition to the Common Criteria evaluation.

5. As Fortinet FortiOS 4.0 MR3 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).

6. Agencies must configure Fortinet FortiOS 4.0 MR3 to conform to the Internet Protocol Security controls in the ISM.

7. Agencies must use the approved FIPS-CC firmware release.

8. Agencies must configure Fortinet FortiOS 4.0 MR3 to use FIPS-CC mode. Further information on operation in FIPS-CC mode is available in the FortiOS Certification and Compliance guide, available from http://docs.fortinet.com/fgt/handbook/40mr3/fortigate-compliance-40-mr3.pdf.

9. Agencies should disable remote management on the external interface. Management tasks should be performed from the internal network or over the VPN. Ideally this should be performed over a dedicated management interface.

10. 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.

11. 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.

12. 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 ASD on 1300 CYBER1 (1300 292 371) or email asd.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.asd.gov.au/infosec/ism/index.htm

Consumer Guide

This Consumer Guide was issued on 29 August 2013 and updated on 27 June 2016.