Maintenance Report

Fortinet FortiGate-VM Unified Threat Management Solutions and FortiOS 4.0 MR3 CC Compliant Firmware

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-7-92-MR
Version: 1.0
Date: 29 July 2013
Pagination: 1 to 2

1 Introduction

Fortinet, Incorporated has submitted (via EWA-Canada) the Impact Analysis Report (IAR) for Fortinet FortiGate-VM Unified Threat Management Solutions and FortiOS 4.0 MR3 CC Compliant Firmware (hereafter referred to as Fortigate-VM FortiOS 4.0), satisfying the requirements outlined in Assurance Continuity: CCRA Requirements, v2.1, June 2012. In accordance with those requirements, the IAR describes the changes implemented in Fortigate FortiOS 4.0, (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

2 Description of changes in the Maintained Target of Evaluation

The following characterizes the changes implemented in Fortigate-VM FortiOS 4.0. For each change, it was verified that there were no required changes to the security functional requirements in the ST, and thorough functional and regression testing was conducted by the developer to ensure that the assurance in the Target of Evaluation (TOE) was maintained. The changes in Fortigate-VM FortiOS 4.0 comprise;

- The TOE has been virtualized as 5 different platforms;
    - FortiGate-VM00
    - FortiGate-VM01
    - FortiGate-VM02
    - FortiGate-VM04
    - FortiGate-VM08
- bug fixes resulting from defects detected and resolved through the QA/test process;
- Pre-shared key length extended to 128 characters; and
- FIPS-CC mode command enabled for virtual platforms.

3 Description of Changes to the IT Environment

As the TOE now has virtual platforms, a VMware ESX/ESXi Server (hypervisor) has been added to the IT environment to host.

4 Affected developer evidence

Modifications to the product necessitated changes to a subset of the developer evidence that was previously submitted for the TOE. The set of affected developer evidence was identified in the IAR.

Modifications to the security target were made to reflect the new product versions.

5 Additional assurance activities

The evaluator performed all setup/installation procedures for the new platforms as they differed from the originally evaluated setup/installation procedures to confirm that they are correct and accurate.

6 Conclusions

All changes to the maintained TOE were bug fixes and performance improvements to the cryptographic module. Through functional and regression testing of Fortigate-VM FortiOS 4.0, assurance gained in the original TOE certification was maintained. As all of the changes to the maintained TOE have been classified as minor, it is the conclusion of the CB that the maintained TOE is appropriate for assurance continuity and re-evaluation is not required.

7 References

- Assurance Continuity: CCRA Requirements, v2.1, June 2012.
- CCS Guide #6, Technical Oversight for Assurance Continuity of a Certified TOE, v1.6, May 2011.
- EAL 4+ Evaluation of Fortinet, Incorporated Fortinet FortiGate™ Unified Threat Management Solutions and FortiOS 4.0 CC Compliant Firmware Evaluation number: 383-4-133 CR Version: 1.0 CR Date: 23 January 2012