Maintenance Report

Fortinet FortiGate™ 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: 383-7-105-MR
Version: 1.0
Date: 29 January 2014
Pagination: 1 to 2

1 Introduction

Fortinet, Incorporated has submitted (via EWA-Canada) the Impact Analysis Report (IAR) for Fortinet FortiGate™ Unified Threat Management Solutions and FortiOS 4.0 MR3 CC Compliant Firmware (hereafter referred to as Fortigate 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 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 FortiOS 4.0 consist of several bug fixes resulting from defects that were detected and resolved through the QA/test process, detailed below:

- Correction of status for SNMP VPN Tunnel monitoring reports;
- Adding continuous self-test to the RNG seed;
- Fixing corruption of config files after some CRLs are loaded;
- Ensuring that when 2 simultaneous phase 1 security associations (SAs) exist, both SAs do not expire without rekeying; and
- Amendment of the Config file so that Config changes are properly saved after the TOE is rebooted.

3 Description of Changes to the IT Environment

There were no changes to the underlying IT environment.

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 Conclusions

All changes to the maintained TOE were bug fixes and performance improvements to the cryptographic module. Through functional and regression testing of Fortigate 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.

6 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 Document number: 383-4-133-CR, v 1.0, 23 January 2012.