



Maintenance Report

Trend Micro Deep Security 8.0 SP1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment, 2012

Document number: 383-7-79-MR
Version: 1.0
Date: 10 August 2012
Pagination: 1 to 2

1 Introduction

Trend Micro Inc. has submitted via EWA-Canada the Impact Analysis Report (IAR) for Trend Micro Deep Security 8.0 SP1, satisfying the requirements outlined in Assurance Continuity: CCRA Requirements, v2.0, November 2011. In accordance with those requirements, the IAR describes the changes implemented in Trend Micro Deep Security 8.0 SP1, (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 Trend Micro Deep Security 8.0 SP1. 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 Trend Micro Deep Security 8.0 SP1 comprise bug fixes resulting from defects detected and resolved through the QA/test process.

3 Description of Changes to the IT Environment

The following additional platforms are supported for the Deep Security Virtual Appliance:

- VMware vCenter 5.0.0; and
- ESXi 5.0.

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 updated TOE version and updated build numbers for the Deep Security Agent, Deep Security Virtual Appliance and Deep Security Filter Driver. The additional platforms for the Deep Security Virtual Appliance are also listed.

5 Conclusions

All changes to the maintained TOE were bug fixes and support for the new platforms. Through functional and regression testing of Trend Micro Deep Security 8.0 SP1, 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, v2.0, November 2011.

CCS Guide #6, Technical Oversight for Assurance Continuity of a Certified TOE, v1.6, May 2011.

Certification Report EAL 4+ Evaluation of Deep Security 7.5 SP2, v1.0, 2 September 2011.