Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA MAINTENANCE REPORT

Tripwire Enterprise Version 8.9.1

10 August 2022

500-EWA

Canada

FOREWORD

This Maintenance Report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The IT product identified in this report has been previously evaluated at an approved Common Criteria testing lab established under the Canadian Common Criteria program using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5.

This report is not an endorsement of the IT product by the Canadian Centre for Cyber Security, and no warranty of the IT product by the Canadian Centre for Cyber Security is expressed or implied.

If your organization has identified a requirement for this maintenance report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

TABLE OF CONTENTS

1 INTRODUCTION

An Impact Analysis Report was submitted to the Canadian Common Criteria program to extend the validity of the Common Criteria certificate previously awarded to **Tripwire Enterprise Version 8.8.2.2** from **Tripwire, Inc.**

The process to achieve this under mutual recognition is described in Assurance Continuity: CCRA Requirements, version 2.1, June 2012. In accordance with the requirements of this process, the Impact Analysis Report describes all changes made to the product and/or its IT environment, all resulting changes made to the evaluation evidence, and the security impact of the changes.

The purpose of this document is to summarize and present the Canadian Common Criteria program's findings regarding the assurance maintenance of **Tripwire Enterprise Version 8.9.1**, hereafter referred to as the maintained Target of Evaluation, or maintained TOE.

2 DESCRIPTION OF CHANGES

The following characterizes the changes implemented in the maintained TOE and/or the environment. For each change, it was verified that there were no required changes to the security functional requirements in the Security Target.

Table 1: TOE Identification

Original TOE	**Tripwire Enterprise Version 8.8.2.2**
Maintained TOE	**Tripwire Enterprise Version 8.9.1**
Developer	**Tripwire, Inc.**

2.1 DESCRIPTION OF CHANGES IN THE MAINTAINED TARGET OF EVALUATION

The changes in the maintained TOE comprise the following:

- Security Patches to address the following CVEs:
  - CVE-2015-2156, CVE-2019-10797, CVE-2019-16869, CVE-2019-20444, CVE-2016-9878, CVE-2018-11039, CVE-2018-1104, CVE-2018-10237, CVE-2015-5237, CVE-2015-7559, CVE-2018-11775, CVE-2019-0222, CVE-2020-1941, CVE-2020-1695, CVE-2018-1000632, CVE-2020-10683, CVE-2017-3523, CVE-2017-3589, CVE-2018-3258, CVE-2019-2692, CVE-2020-2875, CVE-2020-2933, CVE-2020-2934, CVE-2018-1000180, CVE-2018-1000613, CVE-2016- 1000352, CVE-2016-1000346, CVE-2016-1000345, CVE-2016-1000341, CVE-2016- 1000340, CVE-2016-1000339, CVE-2016-1000338, CVE-2017-13098, CVE-2020-11998, CVE-2020-10672, CVE-2020-10673, CVE-2020- 10968, CVE-2020-10969, CVE-2020-11111, CVE-2020-11112, CVE-2020-11113, CVE- 2020-11619, CVE-2020-11620, CVE-2020-14060, CVE-2020-14061, CVE-2020-14062, CVE-2020-14195, CVE-2015-5237, CVE-2016-4000, CVE-2020-15522, CVE-2020-8022, CVE-2020-17527, CVE-2021-41303, CVE- 2020-1957, CVE-2020-13933, CVE-2016-4437, CVE-2014-0074, CVE-2016-6802, CVE-2020-17523, CVE-2020-11989, CVE-2021-23899, CVE-2020-13973, CVE-2021-23900, CVE-2016-1000027, CVE-2021-4104, CVE-2019-17571, CVE-2021-28490
- Removed support for TLS 1.0 & TLS 1.1
- Supported cipher suites changed to:
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
  - TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- Feature enhancements addressing non-SFR related functionality
- Bug fixes to address issues raised during internal QA and external flaw reporting

2.2 DESCRIPTION OF CHANGES TO THE IT ENVIRONMENT

The changes to the IT environment comprise the following:

- Support for Oracle MySQL changed from v5.7.16 to 8.0
- Support for Microsoft Internet Explorer 11 changed to Microsoft Edge 90
- Support for Mozilla Firefox v66 changed to Mozilla Firefox v68
- Amazon Linux no longer supported

2.3 AFFECTED DEVELOPER EVIDENCE

Modifications to the product necessitated changes to the following developer evidence that was previously submitted in support of the original evaluation:

- Tripwire Enterprise Version 8.9.1 User Guide
- Tripwire Enterprise Version 8.9.1 Reference Guide
- Tripwire Enterprise Version 8.9.1 Installation & Maintenance Guide
- Tripwire Enterprise Version 8.9.1 Hardening Guide
- TE Console 8.9.1 Release Notes – June 2022
- Axon Agent and TE Agent Release Notes – June 2022
- Tripwire Enterprise v8.9.1 Supplemental Common Criteria Guidance, Version 1.0, Release Date 14 July 2022
- Tripwire, Inc. Tripwire Enterprise Version 8.9.1 Security Target, Version 1.1,10 August 2022
- Tripwire, Inc. Tripwire Enterprise Version 8.9.1 Life Cycle Document, Version 1.0, 14 July 2022
- Tripwire, Inc. Tripwire Enterprise Version 8.9.1 Design Document, Version 1.0, 14 July 2022

3 CONCLUSIONS

Through functional and regression testing of the maintained TOE, assurance gained in the original TOE certification was maintained. As all 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 maintenance and re-evaluation is not required.

The assurance maintenance of the TOE has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions are consistent with the evidence adduced. This is not an endorsement of the IT product by the Cyber Centre or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the Cyber Centre or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

4 REFERENCES

Reference
Assurance Continuity: CCRA Requirements, v2.1, June 2012
Certification Report Tripwire Enterprise Version 8.8.2.2, 3 September 2020, v1.0
Security Target Tripwire Enterprise Version 8.9.1, 10 August 2022, v1.1
Impact Analysis Report Tripwire Enterprise Version 8.9.1, 10 August 2022, v1.0