Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

COMMON CRITERIA MAINTENANCE REPORT

Dell EMC™ Unity® OE v5.0

20 August 2019

383-7-160

V1.0

Canada

FOREWORD

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

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

Contact Centre and Information Services
Edward Drake Building
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)
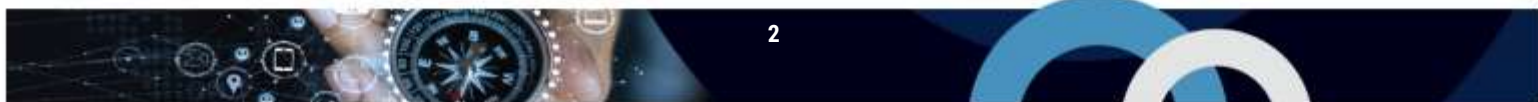
OVERVIEW

This is a Maintenance Report for Dell EMC™ Unity® OE v5.0 (hereafter referred to the TOE), that satisfies the requirements outlined in Assurance Continuity: CCRA Requirements, v2.1, June 2012. In accordance with those requirements, an Impact Assessment Report was submitted which describes the changes implemented in the TOE, (the maintained Target of Evaluation), the evidence updated as a result of the changes and the security impact of the changes.

TABLE OF CONTENTS

1   CHANGES

The following characterizes the changes implemented in the TOE and/or the environment. 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 and the evaluation facility to ensure that the assurance in the Target of Evaluation (TOE) was maintained.

1.1   DESCRIPTION OF CHANGES IN THE MAINTAINED TARGET OF EVALUATION

The changes in the TOE comprise;
- Various bug fixes and feature enhancements resulting from defects detected and resolved through the QA/test process that do not affect the existing security features of the TOE;
- Removal of the 300, 400, 500, 600 hardware models; and
- Support was added for the addition of the 380/F, 480/F, 680/F, and 880/F hardware models.

1.2   DESCRIPTION OF CHANGES TO THE IT ENVIRONMENT

The changes to the IT environment comprise;
- The management workstation changed from Windows Server 2008 R2 SP1 to Windows Server 2016;
- The Active Directory Server changed from Windows Server 2012 R2 to Windows Server 2016; and
- The NIS Server used in NFS authentication was changed from SLES 11 SP3 to SLES 12 SP1.

1.3   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, changes to the operational environment, and the removal/addition of hardware platforms.

2   CONCLUSIONS

Through functional and regression testing of the TOE, 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.

The IT product identified in this report has been previously evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4.

This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

2.1   REFERENCES

Reference
Assurance Continuity: CCRA Requirements, v2.1, June 2012
Certification Report for Dell EMC™ Unity™ OE v4.2.0, v1.0, 22 September 2017
DellEMC™ Unity® OE v5.0Security Target, v1.0, 20 July 2019