Communications Security Establishment Centre de la sécurité des télécommunications

COMMON CRITERIA MAINTENANCE REPORT

CA Privileged Access Manager v2.8.2

383-7-138

July 10, 2017

1.1

Canada

FOREWORD

This Maintenance Report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

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

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

CA, Inc. has submitted the Impact Analysis Report (IAR) for CA Privileged Access Manager v2.8.2 (hereafter referred to the TOE), 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 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 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;

- The hardware model identifier for the TOE has been changed from the Xceedium Stock Keeping Unit (SKU) number to the CA SKU. The X304 L is now identified as the CA HAH 995;

- The following Hotfixes have been applied;
    - 2.7.0.02 Hotfix
    - 2.7.0.05 Hotfix
    - 2.7.0.06 Hotfix
    - 2.7.0.07 Hotfix
    - 2.7.0.08 Hotfix
    - 2.7.0.09 Hotfix
    - 2.7.1.01 Hotfix
    - 2.8.0.01 Hotfix

- The Solid State Drives (SSDs) in the TOE have been upgraded to Intel S3520 240GB SSDs;

- A Cross site scripting (XSS) vulnerability has been addressed;

- CVE-2016-2108 has been addressed; and

- 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 of TOE

1.2   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.

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 CA Privileged Access Manager v2.5.5, v1.0, 26 April 2016
Security Target CA Privileged Access Manager v2.8, v2.1, 10 July 2017