CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8070 (HCDPP)

Maintenance Report Number: CCEVS_VR_VID10955_2019

Date of Activity: 9 December 2019

References:

Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 3.0, September 12, 2016

NIAP Policy #12 “Acceptance Requirements of a product for NIAP Evaluation.” March 20, 2013

Common Criteria document CCIMB-2004-02-009 “Assurance Continuity: CCRA Requirements” Version 1, February 2004

Xerox Multi-Function Device Security Target Xerox® AltaLink C8030 / C8035 / C8045 / C8055 / C8070 Document Version 0.9 (October 2019)

Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8070 VID10955 Maintenance Update Impact Analysis Report October 21, 2019

Affected Evidence:

Xerox Multi-Factor Device Security Target Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8070 Document Version 0.9 (October 2019)

Affected Developer Evidence:

No developer evidence was changed.

Description of ASE Changes:

There are over 60 minor changes to the TOE that are comprised of bug fixes that are included in updates and patches to Xerox® AltaLink™ since certification. Most of the bug fixes are related to Energy Star and California State Law default password changes. Several OpenSSL

vulnerabilities have also been addressed (see DAR-347405) – critically, the underlying FIPS Object Module and related CAVP certificates remain unchanged. Other changes address audit long inconsistencies, cross site scripting problems, and incorrect test results.

Description of ALC Changes:

Changes to the Security Target revision were made, going from version 0.7 to 0.9 with the addition of Software Patch 417710v1.dlm with Release 101.008.019.20200. No other documentation was affected.

Assurance Continuity Maintenance Report:

- Xerox submitted an Impact Analysis Report (IAR) for the Xerox Multi-Factor Device Security Target Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8070.
- This Impact Analysis Report (IAR) documents the analysis of a certificate update. A software patch has been issued for the TOE software fix bugs related to Energy Star and California State Law default password change, OpenSSL vulnerabilities, audit log inconsistencies, cross site scripting problems, and incorrect test results. The IAR indicates that the impact of all the individual changes is minor so it concludes that the sum of all the changes to the TOE have only minor impact.
- The IAR lists the changes to the product with resulted in the creation of Software Patch 417710v1.dlm with Release 101.008.019.20200.
- There are no changes to the IT Environment
- There are no changes to the Development Environment
- Changes to the Security Target are as follows:
  - Document version
  - Copyright year
  - Firmware version
  - OpenSSL version in TOE Summary Specification section 6.1.6 (**Note:** OpenSSL FIPS Object Module version remains the same)
- The CI List was updated with the new Security Target revision. No other documentation was affected
- The Protection Profile is unchanged with no Technical Decisions released since the prior Assurance Maintenance. No changes have been made to the hardware of the TOE models; the model names and manufacturing numbers remain the same. The assurance activity coverage is unchanged. The only changes are the bug fixes and security patches.

Description of Regression Testing:

A full suite of regression tests was performed by Xerox to verify all changes included in the patch to verify there are no changes to the results when compared to the original validation. The regression tests are the same HCD PP Assurance Activity tests conducted by the lab during the

original validation. The same test plan used during the original validation was reused for the regression tests.

Vulnerability Assessment:

Xerox maintains a security advisory service covering the TOE models at https://security.business.xerox.com/en-us/products/altalink-b8000-series/. The changed TOE software addresses all known public security vulnerabilities. Xerox asserts that there are no known public vulnerabilities in the changed TOE as at October 21, 2019.

Vendor Conclusion:

The IAR concludes that all changes to the TOE are *minor* and the overall impact to the TOE is *minor*. It is the conclusion of this report that assurance has been maintained in the changed TOE.

Validation Team Conclusion:

The Validation team has reviewed the changes and concurs that the changes are minor and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. Therefore, CCEVS agrees that the original assurance is maintained for the above cider version of this product.