CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

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

Maintenance Report Number: CCEVS-VR-VID10788-2018

Date of Activity: 6 June 2018

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 2.0 (May 2018)

Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8070 VID10788 Maintenance Update Impact Analysis Report June 7, 2018

Affected Evidence:

Xerox Multi-Factor Device Security Target Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8070 Document Version 2.0 (May 2018)

Affected Developer Evidence:

All developer evidence remains unchanged

Description of ASE Changes:

The only changes to the Security Target were for firmware version identifiers, Copyright, and ST version.

Description of ALC Changes:

Changes to the Security Target revision were made; no other documentation was affected.

Assurance Continuity Maintenance Report:

- DXC.technology submitted an Impact Analysis Report (IAR) on behalf of Xerox for the Xerox Multi-Factor Device Security Target Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8070.
- The Impact Analysis Report (IAR) documents the analysis of a certificate update. There are 75 bug fixes and changes included in the update. Most of the bug fixes are related to print/scan quality issues and calibration issues. None of these changes have any security relevant impact.
    - There are many bug fixes for issues related to the manufacturing process and for the time the machine is in maintenance mode. Neither of these modes are available to the customer and are not accessible by the customer. Therefore, they do not affect the printers while in the evaluated configuration nor can they be caused by the customer.
    - There are several bug fixes for data loss while in transit to or from the TOE. These are not security relevant as there are no SFR claims requiring data to successfully transmit. The only SFR claims are
        1) that data is not transmitted in the clear,
        2) that data is secured while stored on the printer, and
        3) that data is not accessible to unintended parties.
    - There are two changes related to the USB CAC readers but the changes did not affect the security of the Smart Card authentication and did not expose the Local UI to unintended access.
    - There are many changes to parts of the printer that are disabled in the evaluated configuration (i.e., Airprint, Remote UI, etc.) and are, therefore, not relevant as there no claims in the Security Target for these features.
    - The only change that had possible security relevance is Change #35, where a super-imposed image of two previous copy jobs was on a Scan to Email job. This was a bug fix and no changes to the implementation of the relevant SFRs were required. The bug itself was not intentionally reproducible and could not be reproduced except under specific conditions.
- The IAR contains a brief description of the 75 changes and a statement as to its security relevance.
- Section 6 Assurance Activity Coverage Argument of the IAR identifies the three additional Technical Decisions that have been added since the original PCL posting and explains why none are relevant.

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.

The DXC.technology Common Criteria Lab also redid a subset of the regression tests to verify that there are no changes to the security functionality or implementation when compared to the original certification. These are the same tests conducted during the original validation. The lab actual test results matched both the vendor test results and the test results from the original validation.

The DXC.technology Common Criteria Lab regression tests focused on:

a) CAC card enablement and authentication and associated auditing;

b) IPSec and TLS Protocol testing;

c) Local and Network Authentication;

d) Security attribute management;

e) Access Control Security Policy management;

f) Purge data.

Vulnerability Assessment:

A new vulnerability search was conducted on June 6, 2018 with no new vulnerabilities found. The same searches conducted during the original validation were repeated using the same search terms: Xerox, C8030, C8035, C8045, C8055, C8070. Searched were conducted at http://www.securityfocus.com/bid, http://www.kb.cert.org/vuls/, and https://nvd.nist.gov/vuln/search/results?adv_search=false&form_type=basic&results_type=overview&search_type=all&query=xerox.

Additionally, the TOE is not susceptible to the Spectre and Meltdown CPU vulnerabilities. Just-in-time (JIT) compilation is turned off in the Intel CPU.

Vendor Conclusion:

There are no changes to the TOE, thus the ST and the design documentation provided under the original certification are not affected. The assurance baseline is assessed as *minor* within the allowance of the Assurance Continuity framework. 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 cited version of this product.