CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD

Maintenance Report Number: CCEVS-VR-VID11150-2023

Date of Activity: August 3 2023

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." 29 August 2014.

Common Criteria document 2012-06-01 "Assurance Continuity: CCRA Requirements" version 2.1, June 2012

Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-001

Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-002

Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, version 3.1, Revision 5, CCMB-2017-004-003

Protection Profile for Hardcopy Devices, version 1.0, September 10, 2015

Xerox Multi-Function Device Security Target Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with HDD, version 1.1, June 2023

Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD VID11150 Impact Analysis Report #2, version 1.1, July 2023

Affected Evidence

Xerox Multi-Function Device Security Target Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with HDD, version 1.1, June 2023

Updated Developer Evidence

All developer evidence remains unchanged except as noted in this section.

Evidence Identification	Effect on Evidence/ Description of Changes
Xerox Multi-Function Device Security Target Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with HDD, Version 0.8, August 2021	**Maintained Security Target:** Xerox Multi-Function Device Security Target Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with HDD, Version 1.1, June 2023 Changes in the maintained ST are: • Document version and date • Software version update • Table 2 updated to show full model to software version mapping

Description of Changes

The changes made to the Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD since the previous Assurance Maintenance Activity in September 2021 (CCEVS-VR-VID11150-2021) are described here.

- The Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD system software was updated from versions 111.011.011.12103 and 111.013.011.12103 to versions 111.009.003.11600, 111.010.003.11600, 111.011.003.11600, 111.013.003.11600, and 111.014.003.11600.
    - The software updates included non-security relevant features and bug fixes that have no design or functional impact. The software updates and their effects and relevance are summarized below.
- ST updated to show the full breakdown of firmware versions, to include added reference to firmware versions for AltaLink™ C8130 / C8135 (111.009.003.11600), AltaLink™ C8145 / C8155 (111.010.003.11600), and AltaLink™ B8170 (111.014.003.11600). (See section Equivalency Discussion)

Changes to the TOE

The software update address non-security relevant aspects of the Multi-Function Devices (MFDs) described in the table below.

Xerox Ref	Summary	TSF Impact
DAR-719947	SB20-286 CVE-2020-25641- A flaw was found in the Linux kernel's implementation of biovecs in versions before 5.9-rc7. A zero-length biovec request issued by the block subsystem could cause the kernel to enter an infinite loop, causing a denial of service. This flaw allows a local attacker with basic privileges to issue requests to a block device, resulting in a denial of service.	Vulnerability patch. No design or functional impact.

Xerox Ref	Summary	TSF Impact
DAR-719948, DAR-719949	SB20-342 CVE-2020-29369 CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') An issue was discovered in mm/mmap.c in the Linux kernel before 5.7.11. There is a race condition between certain expand functions (expand_downwards and expand_upwards) and page-table free operations from an munmap call, aka CID-246c320a8cfe. SB20-139 CVE-2019-20795 Detail iproute2 before 5.1.0 has a use-after-free in get netnsid_from_name in ip/ipnetns.c.	Vulnerability patch. No design or functional impact.
DAR-719952	SB21-144 Security (NIST 2.9) SB21-144 CVE-2020-24588 CVE-2020-24587 (WiFi) CVE-2020-24588 The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SSP A-MSDU frames (which is mandatory as part of 802.11n), an adversary can abuse this to inject arbitrary network packets. CVE-2020-24587 The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that all fragments of a frame are encrypted under the same key. An adversary can abuse this to decrypt selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP encryption key is periodically renewed.	Vulnerability patch. No design or functional impact. Wireless is disabled.
DAR-720730	Statuses are set and not cleared after clearing the Jam by IIT. When a jam occurs in the top of the DADH for Corvo/Kiska mid/Low, LUI graphics are displayed same as high. Mid/Low devices are displaying High machine graphics in LUI.	Bug fix. No design or functional impact.
DAR-720732	"Doorbell failure" and "Doorbell reject",triggers incorrect faults. While referring RAP manual for Verifying the Fault Codes Specific to CORVO/KISKA in eDoc, RAP is incorrect for "62.792.00: Side 1 doorbell failure", "62.790.00: Side 1 doorbell reject". The fix is to correct that.	Bug fix. No design or functional impact.
DAR-721216	Security Fixes for web injection defect. EIP iconUri parameters were not validated.	Vulnerability patch. No design or functional impact.

Xerox Ref	Summary	TSF Impact
DAR-722129	Due to component shortage we need to enable Realtek RTL8211F-CG for Corvo/Kiska Cougar v1.6.5 Impacted S/S OS team -- OS has to enable the Driver. Ensure we can detect which chip is installed and load the correct driver.	Replacement of physical layer Ethernet chip. No design or functional impact.
DAR-723511	Port to D.5.1 SWUP (software upgrade) code to support Scanner Maxim chip. Part of Maxim chip support.	Scanner chip software update – no TSF relevance. No design or functional impact.
DAR-726052	Security fix for unauthenticated access to the Properties Page which was possible for the Guest User via Cross-site request forgery.	Vulnerability patch. No design or functional impact. **Note:** Guest User is disabled in the evaluated configuration.
DAR-728065	Add the HW Configuration (Maxim, Realtek) info to SBC Name. This information is included in the ConfigSettings.xml retrieved by Remote Services.	No impact. Remotes Services (SMart eSolutions) is disabled in the evaluated configuration.
DAR-734982	Security LDAP Password not Expunged so it can be stolen (Secure LDAP (LDAP over TLS is OK) Fix is to expunge password when new credentials entered.	Vulnerability patch. No design or functional impact. Evaluated configuration uses LDAP over TLS which was not affected.
DAR-735333	The ECDSA Xerox Generic Root CA is not displaying under Server validation for IPSec IKE auth with Digital Certs.	None – evaluated configuration on supports RSA and Pre-shared leys.
DAR-737423	Support Cudy WiFi dongle. The change involves adding the Cudy vendor and product ID to connControl and OS udev rule, so that the dongle can be recognized.	No impact – dongle use outside of the evaluated configuration.

Xerox Ref	Summary	TSF Impact
DAR-737741	Normal print Job went for Paused state. LUI didn't prompted to replace a Magenta toner, but in EWIS notified that" The Magenta Toner (M) is empty. User intervention is required to replace the Magenta Toner (M). LUI must display the prompt to replace toner. " The Magenta Toner (M) is empty. User intervention is required to replace the Magenta Toner (M).	Bug fix. No design or functional impact.
DAR-737753	20us ARM reset done by Copy Controller Software when it starts up. During PowerOn assert iitPltnReset for 3 seconds to remove 24V power	Bug fix. No TSF impact - The ARM auxiliary processor manages the scanner portion of the image path.
DAR-746336	HTML injection Vulnerability found in Workflow scanning/ Header tag should not reflect in the browser, and it should not accept the invalid charters. Burpsuite, webinspect detected.	Vulnerability patch. No design or functional impact.
DAR-746405	https://<IP address>/web_srvc/applicationTestResults.php is vulnerable to XSS	Vulnerability patch. No design or functional impact.

Equivalency Discussion

Firmware Equivalency

No functionality, as defined in the SFRs, was impacted by the Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD versions 111.009.003.11600, 111.010.003.11600, 111.011.003.11600, 111.013.003.11600, and 111.014.003.11600 software update.

The functionality of the Xerox® AltaLink™ system software versions 111.009.003.11600, 111.010.003.11600, 111.011.003.11600, 111.013.003.11600, and 111.014.003.11600 update remains the same as prior evaluated version. The added versions are only to reflect the inclusion of the product codes for TOE models that were already included in the original evaluation, but omitted from the ST. The table below depicts the TOE models, versions, and CPU/OS.

Model	Firmware Version	CPU / OS
AltaLink™ C8130 / C8135	111.**009**.003.11600	Intel Atom E3950 (Goldmont) Wind River Linux 9.0
AltaLink™ C8145 / C8155	111.**010**.003.11600	
AltaLink™ C8170	111.**011**.003.11600	
AltaLink™ B8145 / B8155	111.**013**.003.11600	

Model	Firmware Version	CPU / OS
AltaLink™ B8170	111.**014**.003.11600	

All firmware is the same and has the same build version (11600). The 2nd triplet bolded in the table above relates to the MFD model(s) that the firmware is for – this is known within Xerox as the Product Code.

The 'system software set version' (Firmware Version) is the overall system version number. This number uniquely identifies any release distributed to the Field. It is this version number that will be displayed via the printed configuration report, WEB UI and machine status to uniquely identify the software modules and versions that have been installed onto a machine.

The format is as follows:
AAa.PPP.TTY.DDDRR

Legend:

a) AA = Major Architecture Release - Range 00 - 24
b) a = Minor Architecture Release - Range 0 - 9
c) PPP = Product Code (should remain consistent across the lifetime of a given product) Range 00 - 255
d) TT = Train Car ID - Range 00 - 24
e) Y = Year (last digit) - Range 0 - 9
f) DDD = Julian Day of year
g) RR = Revision - Range 00 - 99

All firmware on all models is the same and therefore equivalent. The Product Code identifier in the firmware version number is different due to Xerox internal product management and identification processes. The Product Codes are static once assigned. In this case, the Product Codes are:

a) 009 = Corvo Low Speed Color
b) 010 = Corvo Mid Speed Color
c) 011 = Corvo High Speed Color
d) 013 = Kiska Mid Speed Mono
e) 014 = Kiska High Speed Mono

CAVP Equivalency

No changes have been made to the TOE's Mocana cryptographic module. All referenced CAVP certificates remain valid and unchanged.

Product Changes

For this Assurance Continuity, the change consists of making the following system software version updates.

- From: Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with HDD with System Software version: 111.011.011.12103 and 111.013.011.12103
- To: Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with HDD with System Software version: 111.009.003.11600, 111.010.003.11600, 111.011.003.11600, 111.013.003.11600, and 111.014.003.11600

Changes to the IT Environment

None

Changes to the Development Environment

None

Assurance Continuity Maintenance Report

Lightship Security submitted an Impact Analysis Report (IAR) on behalf of Xerox® for Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD since the previous Assurance Maintenance activity in September 2021 (CCEVS-VR-VID11150-2021).

The Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD system software was updated from versions 111.011.011.12103 and 111.013.011.12103 to versions 111.009.003.11600, 111.010.003.11600, 111.011.003.11600, 111.013.003.11600, and 111.014.003.11600. The software updates included new non-security relevant features and bug fixes.

The new features and bug fixes did not change how the TSF performed, and the TOE continues to implement the TSF in a manner that is consistent with what is defined in the Security Target.

There was no change to the operational environment for the evaluated configuration of the TOE, therefore, the TOE environment presents no impact to the overall assurance maintenance evaluation.

Regression Testing

A suite of regression tests was executed by Xerox to verify the changes included in the updates and ensure the continued correct operation of the TOE. Xerox affirms that the changed TOE continues to operate as expected.

Vulnerability Assessment

Lightship Security performed a search of public information about vulnerabilities found in printing devices and the implemented communication protocol. The search was in accordance with Labgram #116/Valgram #135 - Vulnerability Evidence.

The following public sources were searched on July 27, 2023:

- NIST National Vulnerability Database: https://nvd.nist.gov
- MITRE CVE Search: https://cve.mitre.org/cve/search_cve_list.html
- Xerox Security Information, Bulletins and Advisory Responses: https://security.business.xerox.com/

The search terms listed below were used:

- Xerox AltaLink
- Xerox
- Printer
- Multi-Function Printer
- IPsec
- TLSv1.2 (and TLS 1.2)
- SSH (refined by Libssh2 v1.9.0)
- SFTP
- Wind River Linux

- Mocana

In summary, the IAR contains the output from the vulnerability assessment since the last assurance maintenance activity performed on September 23, 2021. On July 27, 2023, the search of the public domain using the sources above returned 1437 vulnerabilities. No vulnerabilities were found that are applicable to the TOE.

All known public security vulnerabilities are mitigated in the TOE version. Xerox asserts that there are no known exploitable public vulnerabilities in the changed TOE as of the publication date of the IAR.

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. The updated Security Target received minor updates to address the Changed TOE. Therefore, CCEVS agrees that the original assurance is maintained for the above cited version of the product.