CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

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

Maintenance Report Number: CCEVS-VR-VID11150-2021

Date of Activity: November 16, 2021

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 1.0, February 2004

Xerox Multi-Function Device Security Target Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with HDD, Version 1.0, September 2021

Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD VID11150 Impact Analysis Report #1, Version 1.1, November 2021

Description of Changes

The changes made to the Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD since the previous Common Criteria validation report in August 2021 (CCEVS-VR-VID11150-2021) are described here.

- Substitute of non-security relevant scanner hardware.
- The Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD system software was updated from versions 111.011.000.27020 and 111.013.000.27020 to versions 111.011.011.12103 and 111.013.011.12103. The software updates included non-security relevant features and bug fixes for compatibility with the new scanner hardware. The software updates and their effects and relevance are summarized below.

Changes to the TOE

Xerox Ref	Summary	TSF Impact	Rationale
DAR-556911	New IIT v17.15 Binary Fix: Due to a factory fire, we needed to update the scanner software to support new substitute scanner hardware. The code change was to enable the IIT (Scanner) software to recognize which part is installed at power up and use the correct image quality values and controls based on which scanner hardware is installed on the device.	Minor code fix	The update enables the TOE to be compatible with the new hardware. Neither the hardware nor the software makes any changes to the TSF or impacts the TOE's security functions.

Xerox Ref	Summary	TSF Impact	Rationale
DAR-557002	New FPGA v1.24 SW Fix: Update to the FPGA Capella x.00.01.24.0 to D5.3 MC baseline to add support for the new scanner part.	Minor code fix	Similar to DAR-556911, this is a compatibility change and makes no changes to the TSF or impacts the TOE's security functions.
DAR-554540	Wrong Fault /66.396 Fix: Wrong fault was displayed when DADH (power distribution) cable was disconnected or is bad. This can cause confusion to service and lead to wrong part replacement. Fix was to raise the correct fault code 66.396.	Minor code fix	The change to correct the fault code does not affect the TSF or any claimed security functions.
DAR-554551	Wrong Video graphic displayed for Mid/Low speed scanner Fix: Mid/Low devices are displaying High machine graphics in local control panel when a jam occurs. Fix was to use the correct video for the Mid/Low speed model.	Minor code fix	The graphic fix does not affect the TSF or any claimed security functions.

Equivalency Discussion

No functionality, as defined in the SFRs, was impacted by the Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD versions 111.011.011.12103 and 111.013.011.12103 software update.

The functionality of the Xerox® AltaLink™ system software versions 111.011.011.12103 and 111.013.011.12103 update remains the same as prior evaluated version.

The CAVP certificates that applied in the original evaluation still apply to this assurance maintenance as the CPU, Operating System, and Operational Environment remain 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: 111.011.000.27020 and 111.013.000.27020
- To: 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

Changes to the IT Environment

None

Changes to the Development Environment

None

Affected 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 1.0, September 2021 Changes in the maintained ST are: • Document version and date • Software version update

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 Common Criteria evaluation (CCEVS-VR-VID11150-2021).
- The system software needed to be updated due to non-security relevant scanner hardware substitution.
- The Xerox® AltaLink™ C8130, C8135, C8145, C8155, C8170 & B8145, B8155, B8170 with HDD system software was updated from versions 111.011.000.27020 and 111.013.000.27020 to versions 111.011.011.12103 and 111.013.011.12103. The software updates included new non-security relevant features and bug fixes.

Regression Testing

A suite of regression tests was executed by Xerox to verify the changes included in the patch 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 November 5, 2021.

- NIST National Vulnerability Database: https://nvd.nist.gov
- Community (Symantec) Security Community: https://www.securityfocus.com/
- Tenable Network Security: https://www.tenable.com/cve
- Tipping Point Zero Day Initiative: http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid 7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities
- 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
- SSH
- SFTP
- Libssh2 v1.9.0
- Wind River Linux
- Mocana

CVE Product ID	Search Term	Summary	Rationale
CVE-2021-38085	Printer	The Canon TR150 print driver through 3.71.2.10 is vulnerable to a privilege escalation issue. During the add printer process, a local attacker can overwrite CNMurGE.dll and, if timed properly, the overwritten DLL will be loaded into a SYSTEM process resulting in escalation of privileges. This occurs because the driver drops a world-writable DLL into a CanonBJ %PROGRAMDATA% location that gets loaded by printisolationhost (a system process).	N/A—the Cannon TR150 print driver is not part of the TOE.
CVE-2021-23039	IPsec	On version 16.0.x before 16.0.1.2, 15.1.x before 15.1.3, 14.1.x before 14.1.2.8, and all versions of 13.1.x and 12.1.x, when IPSec is configured on a BIG-IP system, undisclosed requests from an authorized remote (IPSec) peer, which already has a negotiated Security Association, can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	N/A—BGI-IP is not part of the TOE.
CVE-2020-36363	TLSv1.2	Amazon AWS CloudFront TLSv1.2_2019 allows TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, which some entities consider to be weak ciphers.	N/A—AWS CloudFront is not part of the TOE.
Several CVEs-see summary	SSH	CVE-2021-1419, CVE-2020-26301, CVE-2021-41393, CVE-2021-41317, CVE-2016-20012, CVE-2021-37173, CVE-2021-28914, CVE-2021-28913, CVE-2021-28912, CVE-2021-28911, CVE-2021-28909, CVE-2021-34718, CVE-2021-27022, CVE-2021-3634, CVE-2021-34565, CVE-2021-34564, CVE-2021-34563, CVE-2021-34562, CVE-2021-34561, CVE-2021-34560, CVE-2021-34559, CVE-2021-33555, CVE-2021-36370, CVE-2021-1592, CVE-2021-38306, CVE-2021-39615, CVE-2021-36282, CVE-2021-36280, CVE-2021-36279, CVE-2021-36278, CVE-2021-21599, CVE-2021-27794, CVE-2021-21567, CVE-2021-38173, CVE-2021-1572	N/A—the CVEs listed all apply to products that are not part of the TOE.

CVE-2021-36370	SFTP	An issue was discovered in Midnight Commander through 4.8.26. When establishing an SFTP connection, the fingerprint of the server is neither checked nor displayed. As a result, a user connects to the server without the ability to verify its authenticity.	N/A—Midnight Commander is not part of the TOE.
CVE-2021-1572	SFTP	A vulnerability in ConfD could allow an authenticated, local attacker to execute arbitrary commands at the level of the account under which ConfD is running, which is commonly root. To exploit this vulnerability, an attacker must have a valid account on an affected device. The vulnerability exists because the affected software incorrectly runs the SFTP user service at the privilege level of the account that was running when the ConfD built-in Secure Shell (SSH) server for CLI was enabled. If the ConfD built-in SSH server was not enabled, the device is not affected by this vulnerability. An attacker with low-level privileges could exploit this vulnerability by authenticating to an affected device and issuing a series of commands at the SFTP interface. A successful exploit could allow the attacker to elevate privileges to the level of the account under which ConfD is running, which is commonly root. Note: Any user who can authenticate to the built-in SSH server may exploit this vulnerability. By default, all ConfD users have this access if the server is enabled. Software updates that address this vulnerability have been released.	N/A—ConfD is not part of the TOE.
Several CVEs-see summary	Printer	CVE-2021-3441, CVE-2021-3704, CVE-2021-3705, CVE-2021-39237, CVE-2021-28416	N/A—all CVEs listed are appliable to HP products which are not part of the TOE.
Several CVEs-see summary	SSH	CVE-2021-41617, CVE-2021-36298, CVE-2021-41117, CVE-2021-31352, CVE-2021-34781, CVE-2021-40119	N/A—the CVEs listed all apply to products that are not part of the TOE.

CVE-2021-31358	SFTP	A command injection vulnerability in sftp command processing on Juniper Networks Junos OS Evolved allows an attacker with authenticated CLI access to be able to bypass configured access protections to execute arbitrary shell commands within the context of the current user. The vulnerability allows an attacker to bypass command authorization restrictions assigned to their specific user account and execute commands that are available to the privilege level for which the user is assigned. For example, a user that is in the super-user login class, but restricted to executing specific CLI commands could exploit the vulnerability to execute any other command available to an unrestricted admin user. This vulnerability does not increase the privilege level of the user, but rather bypasses any CLI command restrictions by allowing full access to the shell. This issue affects Juniper Networks Junos OS Evolved: All versions prior to 20.4R2-S2-EVO; 21.1 versions prior to 21.1R2-EVO; 21.2 versions prior to 21.2R1-S1-EVO, 21.2R2-EVO.	N/A—Juniper Networks Junos OS Evolved is not part of the TOE.

In summary, 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. Therefore, CCEVS agrees that the original assurance is maintained for the above version of this product.