CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

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

Maintenance Report Number: CCEVS-VR-VID10955-2021

Date of Activity: 22 June 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, February 2004

Xerox Multi-Function Device Security Target Xerox® AltaLink C8030 / C8035 / C8045 / C8055 / C8070 Document Version 2.1 (June 2021)

Secure Installation and Operation of your Xerox® Alta Link® B8045 / B8055 / B8065 / B8075 / B8090 Multifunction Printer Xerox® AltaLink® C8030 / C8035 / C8045 / C8055 / C8070 Color Multifunction Printer VERSION 1.8 JUNE 7, 2021

Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8070 VID10955 Impact Analysis Report #2 Version 0.4 June 22, 2021

Affected Evidence:

Xerox Multi-Function Device Security Target Xerox® AltaLink C8030 / C8035 / C8045 / C8055 / C8070 Document Version 2.0 (May 2021)

Secure Installation and Operation of your Xerox® Alta Link® B8045 / B8055 / B8065 / B8075 / B8090 Multifunction Printer Xerox® AltaLink® C8030 / C8035 / C8045 / C8055 / C8070 Color Multifunction Printer VERSION 1.8 JUNE 7, 2021

Affected Developer Evidence:

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

Description of ASE Changes:

Changes to the Security Target (since version 0.9 described in [MR1]) are as follows:

a) Document version
b) Copyright year

c) Remove DXC.technology
d) Firmware version updated with new patch 553131v3.dlm
e) FMT_SMF.1.1 – remove assignment to enable/disable disk encryption (always enabled)

Description of ALC Changes:

The CI List was updated with the new Security Target revision. No other documentation was affected.

Description of AGD Changes:

Changes to the [AGD] (since version 1.7 described in [MR1]) are as follows:

a) Document version
b) Copyright year
c) Remove configuration steps for enabling and disabling data encryption.
d) State that data encryption is enabled by default at the factory and cannot be disabled.

Assurance Continuity Maintenance Report:

- Lightship 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 changes incorporated into Software Patch 553131v3.dlm which addresses public vulnerabilities/CVEs as shown in the table below. 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.
- There are no changes to the IT Environment
- There are no changes to the Development Environment

Table: TOE Changes to address CVEs

CVE Product ID	Summary/Description	TSF Impact/Mitigation
CVE-2019-10881	Xerox AltaLink B8045/B8055/B8065/B8075/B8090, AltaLink C8030/C8035/C8045/C8055/C8070 with software releases before 103.xxx.030.32000 includes two accounts with weak hard-coded passwords which can be exploited and allow unauthorized access which cannot be disabled.	Minor code fix to ensure that the 'Guest' and 'ForceOnBoxLogin' accounts no longer have hard-coded passwords. These users are not available as a login account from any interface. These accounts are internal system accounts with randomly created passwords that are not modifiable by admin and other users.
CVE-2021-28669	Xerox AltaLink B80xx before 103.008.020.23120, C8030/C8035 before 103.001.020.23120, C8045/C8055 before	Minor code fix that removed the ability to set WebUI configuration attributes.

CVE Product ID	Summary/Description	TSF Impact/Mitigation
	103.002.020.23120 and C8070 before 103.003.020.23120 provide the ability to set WebUI configuration attributes without administrative rights.	
CVE-2021-28670	Xerox AltaLink B8045/B8090 before 103.008.030.32000, C8030/C8035 before 103.001.030.32000, C8045/C8055 before 103.002.030.32000 and C8070 before 103.003.030.32000 allow unauthorized users, by leveraging the 'Scan To' Mailbox feature, to delete arbitrary files from the disk.	Minor code fix that removed the ability of unauthorized users to delete arbitrary files from the disk.
CVE-2021-28668	Xerox AltaLink B80xx before 103.008.020.23120, C8030/C8035 before 103.001.020.23120, C8045/C8055 before 103.002.020.23120 and C8070 before 103.003.020.23120 has several SQL injection vulnerabilities.	Minor code fix that removed all SQL server injections.
CVE-2019-18630	On Xerox AltaLink B8045/B8055/B8065/B8075/B8090 and C8030/C8035/C8045/C8055/C8070 multifunction printers with software releases before 101.00x.099.28200, portions of the drive containing executable code were not encrypted thus leaving it open to potential cryptographic information disclosure.	None – This vulnerability is not exploitable in the evaluated configuration. To exploit, an attacker requires physical access and advanced attack techniques to be able to access keys used to create or extract clone files. Further, an attacker would also need admin role access to an MFP in order to download or install one of these clone files. If the attacker is successful in creating and delivering a handcrafted clone file, there is no known way that the device can be exploited by such a clone file.
CVE-2019-18629	Xerox AltaLink B8045/B8055/B8065/B8075/B8090 and C8030/C8035/C8045/C8055/C8070 multifunction printers with software releases before 101.00x.099.28200 allow an attacker to execute an unwanted binary during a exploited clone install. This requires creating a	Minor code fix –. Modified iptables to prevent the ability to run an unexpected binary.

CVE Product ID	Summary/Description	TSF Impact/Mitigation
	clone file and signing that file with a compromised private key.	
CVE-2019-18628	Xerox AltaLink B8045/B8055/B8065/B8075/B8090 and C8030/C8035/C8045/C8055/C8070 multifunction printers with software releases before 101.00x.099.28200 allow a user with administrative privileges to turn off data encryption on the device, thus leaving it open to potential cryptographic information disclosure.	Minor code fix that removed the ability to enable/disable disk encryption. It is enabled at all times and customer cannot disable. ST was updated to remove enable/disable capability from assignment in FMT_SMF.1 (evaluated configuration required disk encryption to be enabled).

Description of 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. In addition, Lightship Security performed additional testing to verify the implemented changes.

Vulnerability Assessment:

Xerox maintains a security advisory service covering the TOE models at https://security.business.xerox.com/en-us/products/altalink-c8000-series/

Public Domain Sources

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 June 16, 2021.

- NIST National Vulnerability Database: https://nvd.nist.gov
- Community (Symantec) Security Community: https://www.securityfocus.com/
- Tenable Network Security: http://nessus.org/plugins/index.php?view=search
- 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/

The search terms listed below were used:

- Xerox AltaLink 8035
- Xerox AltaLink

- Xerox
- Printer
- Multi-Function Printer
- Wind River Linux
- Mocana

Search Results

The search of the public domain using the search sources above returned a number of vulnerabilities. Identified in "Table: TOE Changes to address CVEs", above, are vulnerabilities that are deemed applicable to the evaluation. Xerox has issued the patch 553131v3.dlm to correct the flaws in the product and ensure that identified vulnerabilities are mitigated. The table below lists the vulnerabilities returned by the search that are deemed not applicable to the evaluation.

Table: Vulnerabilities Not Applicable to the Evaluation

CVE Product ID	Description	Rationale
CVE-2021-28672	Xerox Phaser 6510 before 64.65.51 and 64.59.11 (Bridge), WorkCentre 6515 before 65.65.51 and 65.59.11 (Bridge), VersaLink B400 before 37.65.51 and 37.59.01 (Bridge), B405 before 38.65.51 and 38.59.01 (Bridge), B600/B610 before 32.65.51 and 32.59.01 (Bridge), B605/B615 before 33.65.51 and 33.59.01 (Bridge), B7025/30/35 before 58.65.51 and 58.59.11 (Bridge), C400 before 67.65.51 and 67.59.01 (Bridge), C405 before 68.65.51 and 68.59.01 (Bridge), C500/C600 before 61.65.51 and 61.59.01 (Bridge), C505/C605 before 62.65.51 and 62.59.01 (Bridge), C7000 before 56.65.51 and 56.59.01 (Bridge), C7020/25/30 before 57.65.51 and 57.59.01 (Bridge), C8000/C9000 before 70.65.51 and 70.59.01 (Bridge), C8000W before 72.65.51 allows remote attackers to execute arbitrary code through a buffer overflow in Web page parameter handling.	N/A — This vulnerability is specific to Xerox printers other than the Xerox Altalink MFPs.
CVE-2021-28671	Xerox Phaser 6510 before 64.65.51 and 64.59.11 (Bridge), WorkCentre 6515 before 65.65.51 and 65.59.11 (Bridge), VersaLink B400 before 37.65.51 and 37.59.01 (Bridge), B405 before 38.65.51 and 38.59.01 (Bridge), B600/B610 before 32.65.51 and 32.59.01 (Bridge), B605/B615 before 33.65.51 and 33.59.01 (Bridge), B7025/30/35 before 58.65.51 and 58.59.11 (Bridge), C400 before 67.65.51 and 67.59.01 (Bridge), C405 before 68.65.51 and 68.59.01	N/A — This vulnerability is specific to Xerox printers other than the Xerox Altalink MFPs.

CVE Product ID	Description	Rationale
	(Bridge), C500/C600 before 61.65.51 and 61.59.01 (Bridge), C505/C605 before 62.65.51 and 62.59.01 (Bridge), C7000 before 56.65.51 and 56.59.01 (Bridge), C7020/25/30 before 57.65.51 and 57.59.01 (Bridge), C8000/C9000 before 70.65.51 and 70.59.01 (Bridge), C8000W before 72.65.51 have a remote Command Execution vulnerability in the Web User Interface that allows remote attackers with "a weaponized clone file" to execute arbitrary commands.	
CVE-2021-28673	Xerox Phaser 6510 before 64.61.23 and 64.59.11 (Bridge), WorkCentre 6515 before 65.61.23 and 65.59.11 (Bridge), VersaLink B400 before 37.61.23 and 37.59.01 (Bridge), B405 before 38.61.23 and 38.59.01 (Bridge), B600/B610 before 32.61.23 and 32.59.01 (Bridge), B605/B615 before 33.61.23 and 33.59.01 (Bridge), B7025/30/35 before 58.61.23 and 58.59.11 (Bridge), C400 before 67.61.23 and 67.59.01 (Bridge), C405 before 68.61.23 and 68.59.01 (Bridge), C500/C600 before 61.61.23 and 61.59.01 (Bridge), C505/C605 before 62.61.23 and 62.59.11 (Bridge), C7000 before 56.61.23 and 56.59.01 (Bridge), C7020/25/30 before 57.61.23 and 57.59.01 (Bridge), C8000/C9000 before 70.61.23 and 70.59.01 (Bridge), allows remote attackers with "a weaponized clone file" to execute arbitrary commands in the Web User Interface.	N/A — This vulnerability is specific to Xerox printers other than the Xerox Altalink MFPs.
CVE-2021-20679	Fuji Xerox multifunction devices and printers (DocuCentre-VII C7773/C6673/C5573/C4473/C3373/C3372/C2273, DocuCentre-VII C7788/C6688/C5588, ApeosPort-VII C7773/C6673/C5573/C4473/C3373/C3372 C2273, ApeosPort-VII C7788/C6688/C5588, ApeosPort C7070/C6570/C5570/C4570/C3570/C3070/C7070G/ C6570G/C5570G/C4570G/C3570G/C3070G, ApeosPort-VII C4421/C3321, ApeosPort C3060/C2560/C2060/C3060G/C2560G/C2060G, ApeosPort-VII CP4421, ApeosPort Print C5570, ApeosPort 5570/4570/5570G/4570G, ApeosPort 3560/3060/2560/3560G/3060G/2560G, ApeosPort-VII 5021/ 4021, ApeosPort-VII P5021, DocuPrint CP 555 d/505 d, DocuPrint P505 d, PrimeLink C9065/C9070, DocuPrint CP475AP, and DocuPrint P475AP) allow an attacker to cause a denial of service (DoS) condition and abnormal	N/A — This vulnerability is specific to Xerox printers other than the Xerox Altalink MFPs.

CVE Product ID	Description	Rationale
	end (ABEND) of the affected products via sending a specially crafted command.	

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.

References

Ref.	Document
[MR1]	CCEVS Approved Assurance Continuity Maintenance Report - Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8070 (HCDPP) Maintenance Report Number: CCEVS-VR-VID10955-2019 https://www.niap-ccevs.org/MMO/ProductAM/st_vid10955-add1.pdf
[LST]	Xerox VID10955 Assurance Maintenance Test Report Version 0.1, June 2021
[AGD]	Secure Installation and Operation of your Xerox® Alta Link® B8045 / B8055 / B8065 / B8075 / B8090 Multifunction Printer Xerox® AltaLink® C8030 / C8035 / C8045 / C8055 / C8070 Color Multifunction Printer, Version 1.8, June 7, 2021