National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Xerox® AltaLink™ C8130/C8135/C8145/C8155/C8170 &B8145/B8155/B8170 with SSD

Report Number: CCEVS-VR-VID11149-2021

Dated: August 20, 2021

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

James Donndelinger

Meredith Hennan

The Aerospace Corporation

Evaluation Team

Travis Hoffmeister

Eve Pierre

Kevin Steiner

Lightship Security, USA

Table of Contents

List of Tables

1. Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for the end-user with determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment by the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Xerox® AltaLink™ C8130/C8135/C8145/C8155/C8170 & B8145/B8155/B8170 with SSD Target of Evaluation (TOE), performed by Lightship Security USA Common Criteria Laboratory (CCTL). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by Lightship Security (LS) of Austin, Texas in accordance with the United States evaluation scheme and completed in August 2021. The information in this report is largely derived from the ST, and the evaluation sensitive documents: Evaluation Technical Report (ETR) and the functional testing report, which are summarized in the Assurance Activity Report (AAR). The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated April 2017, and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1, Revision 5, April 2017. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and conformant to the Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015 and Errata for the Hard Copy Device Protection Profile v1.0 (PP_HCD_v1.0).

The Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD is a multi-function printer device that copies and prints with scan and fax capabilities.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD System Software version: 111.011.000.27020 and 111.013.000.27020
Sponsor and Developer	Xerox Corporation 800 Phillips Road Rochester, NY 14580
CCTL	Lightship Security 11044 Research Blvd., Suite A-220 Austin, Texas Technology 78759
Completion Date	August 2021
Interpretations	There are the following Technical Decisions for this evaluation. 0562 - Test Activity for Public Key Algorithms 0494 – Removal of Mandatory SSH Cipher Suites for HCD 0474 – Removal of Mandatory Cipher Suite for FCS_TLS_EXT.1 0393 – Require FTP_TRP.1(b) only for printing 0299 – Update to FCS_CKM.4 Assurance Activities 0261 – Destruction of CSPs in flash 0253 – Assurance Activities for Key Transport 0219 – NIAP Endorsement of Errata for HCD PP v1.0 0176 – FDP_DSK_EXT.1.2 - SED Testing 0157 – FCS_IPSEC_EXT.1.1 - Testing SPDs 0074 – FCS_CKM.1(a) Requirement in HCD PP v1.0
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5, April 2017
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Protection Profile	Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015 and Errata for the Hard Copy Device Protection Profile v1.0.

Item	Identifier
Disclaimer	This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.
Evaluation Personnel	Travis Hoffmeister Eve Pierre Kevin Steiner *Lightship Security USA*
Validation Personnel	Jim Donndelinger Meredith Hennan *The Aerospace Corporation*

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Product Compliant List (PCL).

Table 2 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated
- The Security Target (ST), describing the security features, claims, and assurances of the product

Table 2: Evaluation Identifiers

Item	Identifier
ST Title and Version	Xerox Multi-Function Device Security Target, Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD, version 0.6
Publication Date	August 2021
Vendor	Xerox Corporation
ST Author	Xerox Corporation, Erin Huber
Target of Evaluation Reference	Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD
TOE Software Version	111.011.000.27020 and 111.013.000.27020
Keyword	Multi-function Device

3. Security Problem Definition

3.1. Assumptions

The ST identified the following security assumptions contained in Table 3:

Table 3: Secure Usage Assumptions

ID	Assumptions
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

3.2. Threats

The ST identified the following threats addressed by the TOE:

Table 3: Threats Addressed

ID	Threats
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) User Document Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.3. Organizational Security Policies

The Security Target identifies the following Organizational Security Policies (OSPs) to which the TOE must comply.

Table 4: Organizational Security Policies

ID	Organizational Security Policy
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION	If the TOE stores User Document Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of User Document Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.
P.IMAGE_OVERWRITE	Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.
P.PURGE_DATA	The TOE shall provide a function that an authorized administrator can invoke to make all customer-supplied User Data and TSF Data permanently irretrievable from Nonvolatile Storage Devices.

4. Architectural Information

4.1. TOE Evaluated Platforms

The TOE evaluated platforms include the Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8075 with SSD running system software version: 111.011.000.27020 and 111.013.000.27020.

Model	Firmware Version	CPU / OS
AltaLink™ C8130 / C8135 C8145 / C8155/ C8170	111.011.000.27020	Intel Atom E3950 (Goldmont) Wind River Linux 9.0
AltaLink™ B8145 / B8155/ B8170	111.013.000.27020	

4.2. Physical Scope and Boundary

The TOE is an MFD (Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD) that consists of a printer, copier, scanner, fax and associated administrator and user guidance. The TOE comprises the hardware, all software and firmware within the MFD enclosure.

Xerox® AltaLink® B8145/B8155/B8170 are mono MFP or black and white printers; C8130/C8135/C8145/ C8155/C8170 are color MFP or color printers. All models have an Intel Atom E3950 (Goldmont) processor and run WindRiver Linux 9.0. Each model consists of an input document handler and scanner, Xerox embedded Fax accessories, marking engine, controller, Xerox Workflow scanning accessory and user interface. Differences between models is limited to print speed and options such as finishers, paper trays and document handlers. The differences between the models are not security relevant.

4.3. Required Non-TOE Hardware, Software, and Firmware

The TOE does not require any additional hardware, software or firmware in order to function as a multi-function hard copy device. Additional features require that the TOE operates with the following non-TOE components in the environment:

a. IPv4 or IPv6 network environment
b. Publicly Switched Telephone Network (PSTN)
c. LDAP server for authentication services
d. NTP server for time services
e. File server for Workflow Scanning
f. Log server (file server) for remote log storage

g. Printer drivers on supported OS per https://www.support.xerox.com/support/altalink-c8100-series/support/enus.html

h. Smart card authentication requires Federal Information Processing Standard (FIPS) 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smart cards and readers or equivalent. In support of smart card authentication, a Windows Domain Controller must also be present in the environment.

5. Security Policy

The core functionality of the Xerox Multi-Function Device Security Target, Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD is the ability to protect the data transmitted to the multifunction device.

The TOE provides the following security features:

Identification and Authentication

In the evaluated configuration, the TOE requires users and system administrators to authenticate before granting access to user (copy, print, fax, etc.) or system administration functions via the Embedded Web Server (EWS) or the Local User Interface (LUI). The user or system administrator must enter a username and password at either the EWS or the LUI. The password is obscured as it is being entered. The TOE provides role based access control as configured by the system administrator.

The TOE also supports smart card and Lightweight Directory Access Protocol (LDAP) for network authentication.

Security Audit

The TOE generates audit logs that track events/actions (e.g., print/scan/fax job submission) to identified users. The audit logs, which are stored locally in a 15000-entry circular log, are available to TOE administrators and can be exported in comma separated format for viewing and analysis.

Access Control

The TOE enforces a system administrator defined role based access control policy. Only authenticated users assigned to roles with the necessary privileges are allowed to perform copy, print, scan or fax on the TOE via the EWS or the LUI.

Unauthenticated users can submit print or LanFax jobs to the TOE via printing protocols. Release of unauthenticated print jobs to the hardcopy output handler is dependent on the system administrator defined policy.

Security Management

A Local User, via the local user interface, or a Remote User, via EWS, with administrative privileges can configure the security settings of the TOE. The TOE

has the capability to assign Users to roles that distinguish Users who can perform administrative functions from Users who can perform User functions via a role based access control policy. The TOE also has the capability to protect its security settings from unauthorized disclosure and alteration when they are stored in the TOE and in transit to or from the browser-based interface.

Trusted Operation

The TOE includes a software image verification feature and Embedded Device Security which it uses to detect unauthorized modification of TOE software and to verify correct operation of the TOE software.

Encryption

The TOE includes the Mocana cryptographic module software version 6.5.1f which it uses for all in-scope cryptographic operations. The TOE utilizes digital signature generation and verification (RSA), data encryption (AES), key establishment (RSA) and cryptographic checksum generation and secure hash computation (HMAC) in support of disk encryption, SSH, TLS, TLS/HTTPS, TLS/SMTP and IPsec. The TOE also provides random bit generation in support of cryptographic operations.

The TOE stores temporary image data created during a copy, print, scan and fax job on the single shared solid disk drive (SSD). This temporary image data consists of the original data submitted and additional files created during a job. All partitions of the SSD used for spooling temporary files are encrypted. All print scan, and fax jobs are sent over IPSec encrypted channels. The SSD drive encryption key is derived from a BIOS saved passphrase and is the same value for each power-up (see KMD for details).

Trusted Communication

The TOE provides support for a number of secure communication protocols:

- Transport Layer Security (TLS) support is available for protecting communication over the Embedded Web Server (EWS) and SMTP email communications. TLS is also used to protect communication with the remote authentication server (LDAPS)
- Secure Shell (SSH) File Transfer Protocol (SFTP) is available for audit log secure transfers to a remote file repository.
- Internet Protocol Security (IPsec) support is available for protecting communication with print clients and communication with the domain controller when using SmartCard authentication.

PSTN Fax-Network Separation

The TOE provides separation between the fax processing board and the network interface and therefore prevents an interconnection between the PSTN and the internal network. This separation is realized in software, as by design, these interfaces may only communicate via an intermediary.

Data Clearing and Purging

The purge feature allows an authorized administrator to permanently delete all customer-supplied data on the TOE. This addresses residual data concerns when the TOE is decommissioned from service or redeployed to a different environment.

6. Assumptions

The scope of this evaluation was limited to the functionality and assurances covered in the PP_HCD_v1.0 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices need to be assessed separately, and no further conclusions can be drawn about their effectiveness

7. Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the PP_HCD_v1.0 and performed by the Evaluation Team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target in accordance with the PP_HCD_v1.0 and applicable Technical Decisions. All other functionality provided by these devices is not covered by this evaluation and needs to be assessed separately as no further conclusions can be drawn about their effectiveness.
- The following features were not tested as part of the evaluation, and must not be enabled or used for the TOE to be in the evaluated configuration:
    - Reprint from Saved Job
    - SMart eSolutions
    - Custom Services (Extensible Interface Platform or EIP)
    - Network Accounting and Auxiliary Access
    - Internet Fax
    - Embedded Fax mailboxes
    - Wi-Fi Direct Printing
    - Weblet Services
    - InBox Apps
    - Remote Control Panel
    - SFTP when used for scanning
    - SNMPv3

- Scan to USB
- Print from USB
- SMB Filing
- Convenience Authentication
- Xerox Workplace Cloud
- Proximity Card Authentication

8. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Secure Installation and Operation of your Xerox® Alta Link® B8145 / B8155 / B8170 Multifunction Printer, Xerox® AltaLink® C8130 / C8135 / C8145 / C8155 / C8170 Color Multifunction Printer, August 2021, v2.2*
- *Xerox® AltaLink® Series Multifunction Printer System Administrator Guide, February 2021, v2.4*
- *Xerox® AltaLink® B81XX Series Multifunction Printer Multifunction Printer User Guide, May 2020, v1.0*
- *Xerox® AltaLink® C81XX Series Multifunction Printer Multifunction Printer User Guide, May 2020, v1.0*
- *Xerox® AltaLink® Series Smart Card Installation and Configuration Guide, December 2020, v3.0*

All documentation delivered with the product is relevant to and within the scope of the TOE. Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

9. IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 Evaluation Detailed Test Report, v1.1(DTR), as summarized in the evaluation Assurance Activity Report.

9.1. Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

9.2. Evaluation Team Independent Testing

The evaluation team conducted independent testing at Lightship Security USA lab in Austin, Texas. The evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

The TOE testing environment components are identified in Table 5 and Table 6, and diagram of test setup in Figure 1 below. The Secure Installation and Operation of your Xerox AltaLink B8145/B8155/B8170 Multifunction Printer Xerox AltaLink C8130 /C8135, C8145 /C8155/C8170 [SIG] was used to setup and configure the evaluated configuration.

Figure 1: Test Setup

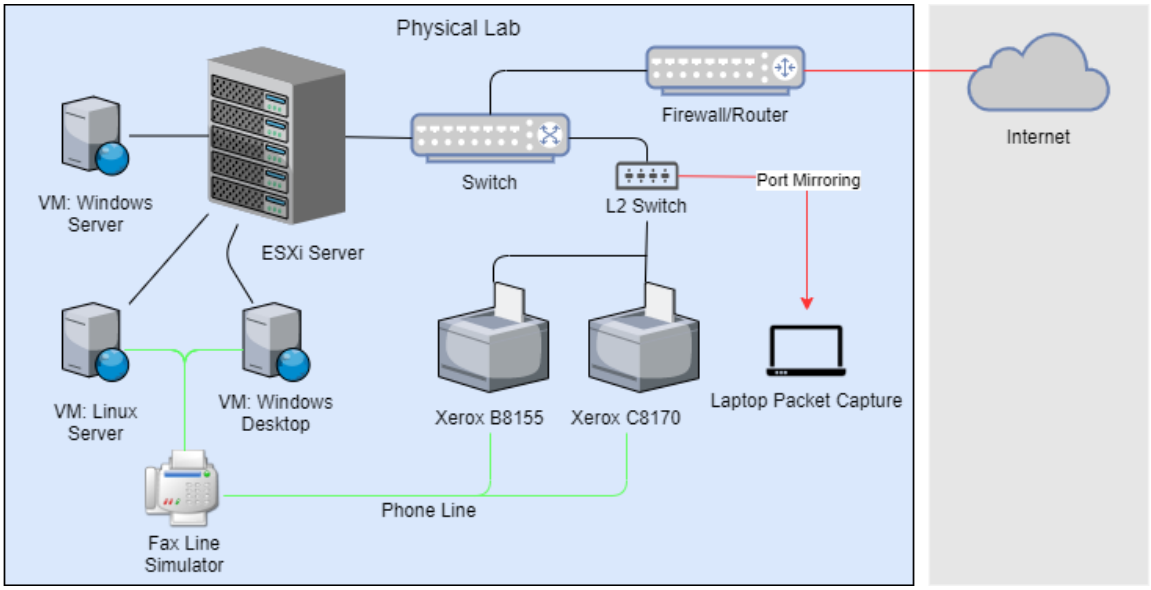

Table 5: Devices in the Testing Environment

Device Name	OS Version	Tools
Windows Server (VM)	Windows Server 2019 Standard Edition	Active Directory, Scan to Mailbox Server, Print Server, Window DNS Server, LDAP server Protocols – Ipsec, TLS
Linux Server (VM)	Linux 4.9.0-13-amd64 Debian 4.9.228-1	NTP, Audit Server, FTP Server, TLS Server, TLS Client, IPsec Endpoint, SSH Client, SSH Server, SMTP.
Windows Desktop	Windows 10	TOE Print Drivers, Fax

ESXi Server	ESXi-6.7.0	Host for all virtual machines
Laptop	Windows 10 Pro	Main laptop used for testing & packet capture. In addition, the Laptop is used to connect to the device to make modifications and perform tests over a serial connection. Protocols - SSH, TLSC, Serial, Fax
Advance Phone Line Stimulator	Viking Model DLE-300	Communication between the TOE and the Window Fax Machine (software) goes over an advanced phone line simulator.
Xerox C8170	111.011.000.27020	TOE Printer

Table 6: Tools Used for Testing

Tool	Version	Tool Location	Tool Purpose
GreenLight	2.2.8	Linux Server (VM)	FCS_TLS_EXT.1 and FCS_SSH_EXT.1 testing
IPSec	strongSwan U5.5.1/K4.9.0-13-amd64	Linux Server (VM)	FCS_IPSEC_EXT.1 testing
Ping	N/A	Linux Server (VM)	FCS_IPSEC_EXT.1 testing
sshd-ls	OpenSSH_7.1p2-Lightship	Linux Server (VM)	FCS_SSH_EXT.1 testing

SNMP	Net-SNMP	Linux Server (VM)	FAU_STG.4 testing
LPR	Part of Windows 10	Windows Desktop (VM)	FDP_ACF.1 testing
Xerox Drivers	Version 7.132.19.0	Windows Desktop (VM)	FDP_ACF.1 and FTP_TRP.1(b)
Wireshark	Version 3.2.6	Laptop	Packet captures throughout testing
Tera Term	Version 4.105	Laptop	FDP_DSK_EXT.1 and FDP_FSX_EXT.1
DNSmasq	Version 2.76	Linux Server (VM)	DNS services
Active Directory	objectVersion 88	Windows Server (VM)	FTP_ITC.1 testing
Cerberus	Version 9.0.5.3	Windows Server (VM)	FCS_SSH_EXT.1 testing
Postfix	Version 3.5.6	Test Services (VM)	FAU_STG.4 testing

10. Evaluated Configuration

The TOE evaluated configuration includes the Xerox® AltaLink™ C8030 / C8035 / C8045 / C8055 / C8075 with SSD running system software version: 111.011.000.27020 and 111.013.000.27020.

Model	Firmware Version	CPU / OS
AltaLink™ C8130 / C8135 C8145 / C8155/ C8170	111.011.000.27020	Intel Atom E3950 (Goldmont) Wind River Linux 9.0
AltaLink™ B8145 / B8155/ B8170	111.013.000.27020	

11. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5, with *Exact Conformance, Selection-Based SFRs, Optional SFRs* CC and CEM addenda, version 0.5, May 2017. The evaluation determined the Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD TOE to be Part 2 extended, and to meet the SARs contained in the PP_HCD_v1.0 and Protection Profile for Hardcopy Devices, Version 1.0 Errata #1.

11.1. Evaluation of the Security Target (ASE)

The Evaluation Team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the Evaluation Team, and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

11.2. Evaluation of the Development (ADV)

The Evaluation Team applied each ADV CEM work unit. The Evaluation Team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the Evaluation Team performed the assurance activities specified in the PP_HCD_v1.0 related to the examination of the information contained in the TSS.

The validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

11.3. Evaluation of the Guidance Documents (AGD)

The Evaluation Team applied each AGD CEM work unit. The Evaluation Team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation Team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

11.4. Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation Team applied each ALC CEM work unit. The Evaluation Team found that the TOE was identified.

The validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

11.5. Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation Team applied each ATE CEM work unit. The Evaluation Team ran the set of tests specified by the assurance activities in the PP_HCD_v1.0 and recorded the results in a Test Report, summarized in the AAR.

The validators reviewed the work of the Evaluation Team and found that sufficient evidence and justification was provided by the Evaluation Team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation Team was justified.

11.6. Vulnerability Assessment Activity (VAN)

The Evaluation Team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator.

On August 3, 2021, the evaluation team performed a search of publicly available information to identify potential vulnerabilities in the TOE using guidelines from Labgram #116/Valgram #135.

The public sources searched included:

- NIST National Vulnerability Database at 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/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities
- Xerox Security Information, Bulletins and Advisory Responses: https://security.business.xerox.com/

The evaluator used the following search terms:

- Xerox AltaLink
- Xerox
- Multi-Function Printer
- Printer
- IPsec
- TLSv1.2
- SSH
- SFTP
- Libssh2 v1.9.0
- Wind River Linux
- Mocana

Based on the results of this effort, there were no identifiable vulnerabilities found at the time of certification.

11.7. Summary of Evaluation Results

The Evaluation Team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation Team's testing also demonstrated the accuracy of the claims in the ST.

The Validation Team's assessment of the evidence provided by the Evaluation Team is that it demonstrates that the Evaluation Team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

12. Validator Comments/Recommendations

All validator comments have been addressed in the Clarification of Scope.

13. Annexes

None

14. Security Target

Xerox Multi-Function Device Security Target, Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD, dated August 2021, Version 0.6

15. Glossary

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

16. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

17. Bibliography

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
4. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
5. Protection Profile for Hardcopy Devices, Version 1.0
6. Protection Profile for Hardcopy Devices, Version 1.0, Errata #1
7. Xerox Multi-Function Device Security Target Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD, v0.6
8. Secure Installation and Operation of your Xerox® Alta Link® B8145 / B8155 / B8170 Multifunction Printer, Xerox® AltaLink® C8130 / C8135 / C8145 / C8155 / C8170 Color Multifunction Printer, v2.2
9. Xerox® AltaLink™ Series Multifunction Printer System Administrator Guide, v2.4
10. Xerox® AltaLink™ B81XX Series Multifunction Printer Multifunction Printer User Guide, v1.0
11. Xerox® AltaLink™ C81XX Series Multifunction Printer Multifunction Printer User Guide, v1.0
12. Xerox® AltaLink™ Series Smart Card Installation and Configuration Guide, v3.0
13. Xerox® AltaLink™ Xerox AltaLink C8130/C8135/C8145/C8155/C8170 & B8145/B8155/B8170 with SSD Evaluation Technical Report, v0.5
14. Xerox® AltaLink™ Printers Key Management Description, version 3.0
15. Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with HDD and SSD Entropy Description, v1.0
16. Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 Evaluation Detailed Test Report, v1.1
17. Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with SSD Assurance Activity Report, v0.4