National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

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

Report Number: CCEVS-VR-VID11150-2021
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

1. Executive Summary ........................................................................................................... 1
2. Identification ..................................................................................................................... 3
3. Security Problem Definition ............................................................................................. 4
   3.1. Assumptions ................................................................................................................ 4
   3.2. Threats ........................................................................................................................ 4
   3.3. Organizational Security Policies ................................................................................. 4
4. Architectural Information .................................................................................................. 6
   4.1. TOE Evaluated Platforms ......................................................................................... 6
   4.2. Physical Scope and Boundary .................................................................................... 6
   4.3. Required Non-TOE Hardware, Software, and Firmware ............................................. 6
5. Security Policy .................................................................................................................. 7
6. Assumptions ...................................................................................................................... 9
7. Clarification of Scope ....................................................................................................... 9
8. Documentation .................................................................................................................. 10
9. IT Product Testing ........................................................................................................... 11
   9.1. Developer Testing ....................................................................................................... 11
   9.1. Evaluation Team Independent Testing ...................................................................... 11
10. Evaluated Configuration ................................................................................................ 14
11. Results of the Evaluation ............................................................................................... 14
   11.1. Evaluation of the Security Target (ASE) ................................................................ 15
   11.2. Evaluation of the Development (ADV) ................................................................ 15
   11.3. Evaluation of the Guidance Documents (AGD) ...................................................... 15
   11.4. Evaluation of the Life Cycle Support Activities (ALC) .......................................... 16
   11.5. Evaluation of the Test Documentation and the Test Activity (ATE) ....................... 16
   11.6. Vulnerability Assessment Activity (VAN) .............................................................. 16
   The Evaluation Team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. ........................................... 16
   11.7. Summary of Evaluation Results .............................................................................. 17
   11.8. Results of the Evaluation ....................................................................................... 17
12. Validator Comments/Recommendations .......................................................................... 17
13. Annexes ......................................................................................................................... 18
14. Security Target ................................................................................................ 19
15. Glossary ........................................................................................................... 20
16. Acronym List ..................................................................................................... 21
17. Bibliography ...................................................................................................... 22

List of Tables

Table 1: Evaluation Details ...................................................................................... 1
Table 2: Evaluation Identifiers ................................................................................ 3
Table 3: Threats Addressed ...................................................................................... 4
Table 4: Organizational Security Policies ............................................................... 5
Table 5: Devices in the Testing Environment ......................................................... 12
Table 6: Tools Used for Testing .............................................................................. 13
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 HDD 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 HDD is a multi-function printer device that copies and prints with scan and fax capabilities.

<table>
<thead>
<tr>
<th>Item</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluated Product</td>
<td>Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 &amp; B8145 / B8155 / B8170 with HDD System Software version: 111.011.000.27020 and 111.013.000.27020</td>
</tr>
</tbody>
</table>
| Sponsor and Developer | Xerox Corporation  
800 Phillips Road  
Rochester, NY 14580 |
<table>
<thead>
<tr>
<th>Item</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCTL</td>
<td>Lightship Security</td>
</tr>
<tr>
<td></td>
<td>11044 Research Blvd., Suite A-220</td>
</tr>
<tr>
<td></td>
<td>Austin, Texas Technology 78759</td>
</tr>
<tr>
<td>Completion Date</td>
<td>August 2021</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interpretations</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are the following Technical Decisions for this evaluation.</td>
</tr>
<tr>
<td>0562 - Test Activity for Public Key Algorithms</td>
</tr>
<tr>
<td>0494 – Removal of Mandatory SSH Cipher Suites for HCD</td>
</tr>
<tr>
<td>0474 – Removal of Mandatory Cipher Suite For FCS_TLS_EXT.1</td>
</tr>
<tr>
<td>0393 – Require FTP_TRP.1(b) only for printing</td>
</tr>
<tr>
<td>0299 – Update to FCS_CKM.4 Assurance Activities</td>
</tr>
<tr>
<td>0261 – Destruction of CSPs in flash</td>
</tr>
<tr>
<td>0253 – Assurance Activities for Key Transport</td>
</tr>
<tr>
<td>0219 – NIAP Endorsement of Errata for HCD PP v1.0</td>
</tr>
<tr>
<td>0176 – FDP_DSK_EXT.1.2 - SED Testing</td>
</tr>
<tr>
<td>0157 – FCS_IPSEC_EXT.1.1 - Testing SPDs</td>
</tr>
<tr>
<td>0074 – FCS_CKM.1(a) Requirement in HCD PP v1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CEM</th>
<th>Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 5, April 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation Scheme</td>
<td>United States NIAP Common Criteria Evaluation and Validation Scheme</td>
</tr>
<tr>
<td>Protection Profile</td>
<td>Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015 and Errata for the Hard Copy Device Protection Profile v1.0.</td>
</tr>
<tr>
<td>Disclaimer</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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>
<thead>
<tr>
<th>Item</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST Title and Version</td>
<td>Xerox Multi-Function Device Security Target, Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 &amp; B8145 / B8155 / B8170 with HDD, version 0.8</td>
</tr>
<tr>
<td>Publication Date</td>
<td>August 2021</td>
</tr>
<tr>
<td>Vendor</td>
<td>Xerox Corporation</td>
</tr>
<tr>
<td>ST Author</td>
<td>Xerox Corporation, Erin Huber</td>
</tr>
<tr>
<td>Target of Evaluation Reference</td>
<td>Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 &amp; B8145 / B8155 / B8170 with HDD</td>
</tr>
<tr>
<td>TOE Software Version</td>
<td>111.011.000.27020 and 111.013.000.27020</td>
</tr>
<tr>
<td>Keyword</td>
<td>Multi-function Device</td>
</tr>
</tbody>
</table>
3. Security Problem Definition

3.1. Assumptions

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

Table 3: Secure Usage Assumptions

<table>
<thead>
<tr>
<th>ID</th>
<th>Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>A PHYSICAL</td>
<td>Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.</td>
</tr>
<tr>
<td>A NETWORK</td>
<td>The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.</td>
</tr>
<tr>
<td>A TRusted ADMIN</td>
<td>TOE Administrators are trusted to administer the TOE according to site security policies.</td>
</tr>
<tr>
<td>A TRAINED USERS</td>
<td>Authorized Users are trained to use the TOE according to site security policies.</td>
</tr>
</tbody>
</table>

3.2. Threats

The ST identified the following threats addressed by the TOE:

Table 3: Threats Addressed

<table>
<thead>
<tr>
<th>ID</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>T UNAUTHORIZED_ACCESS</td>
<td>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.</td>
</tr>
<tr>
<td>T TSF COMPROMISE</td>
<td>An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE’s interfaces.</td>
</tr>
<tr>
<td>T TSF FAILURE</td>
<td>A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.</td>
</tr>
<tr>
<td>T UNAUTHORIZED UPDATE</td>
<td>An attacker may cause the installation of unauthorized software on the TOE.</td>
</tr>
<tr>
<td>T NET COMPROMISE</td>
<td>An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Organizational Security Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>P.AUTHORIZATION</td>
<td>Users must be authorized before performing Document Processing and administrative functions.</td>
</tr>
<tr>
<td>P.AUDIT</td>
<td>Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.</td>
</tr>
<tr>
<td>P.COMMS_PROTECTION</td>
<td>The TOE must be able to identify itself to other devices on the LAN.</td>
</tr>
<tr>
<td>P.STORAGE_ENCRYPTION</td>
<td>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.</td>
</tr>
<tr>
<td>P.KEY_MATERIAL</td>
<td>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.</td>
</tr>
<tr>
<td>P.FAX_FLOW</td>
<td>If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.</td>
</tr>
<tr>
<td>P.IMAGE_OVERWRITE</td>
<td>Upon completion or cancellation of a Document Processing job, the TOE shall overwrite residual image data from its Field-Replaceable Nonvolatile Storage Devices.</td>
</tr>
<tr>
<td>P.PURGE_DATA</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Model</th>
<th>Firmware Version</th>
<th>CPU / OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AltaLink™ C8130 / C8135</td>
<td>111.011.000.27020</td>
<td>Intel Atom E3950 (Goldmont)</td>
</tr>
<tr>
<td>C8145 / C8155/ C8170</td>
<td></td>
<td>Wind River Linux 9.0</td>
</tr>
<tr>
<td>AltaLink™ B8145 / B8155/</td>
<td>111.013.000.27020</td>
<td></td>
</tr>
<tr>
<td>B8170</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.2. Physical Scope and Boundary

The TOE is an MFD (Xerox® AltaLink™ C8130 / C8135 / C8145 / C8155 / C8170 & B8145 / B8155 / B8170 with HDD) 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
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 HDD 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 hard disk drive (HDD) that is field replaceable. This temporary image data consists of the original data submitted and additional files created during a job. All partitions of the HDD used for spooling temporary files are encrypted. The hard drive encryption key is derived from a BIOS saved passphrase and is the same value after each power-up (see KMD for details). All print, fax, and scan jobs occur over IPSec encrypted channels.

**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 Image Overwrite Security feature overwrites temporary image files created during a copy, print, scan or fax job when those files are no longer needed. Overwrite is also invoked at the instruction of a job owner or administrator and at start-up. 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
o Remote Control Panel
o SFTP when used for scanning
o SNMPv3
o Scan to USB
o Print from USB
o SMB Filing
o Convenience Authentication
o Xerox Workplace Cloud
o 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 evaluation team.

9.1. Developer Testing

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

9.1. 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

<table>
<thead>
<tr>
<th>Device Name</th>
<th>OS Version</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux Server (VM)</td>
<td>Linux 4.9.0-13-amd64 Debian 4.9.228-1</td>
<td>NTP, Audit Server, FTP Server, TLS Server, TLS Client, IPsec Endpoint, SSH Client, SSH Server, SMTP.</td>
</tr>
<tr>
<td>Windows Desktop</td>
<td>Windows 10</td>
<td>TOE Print Drivers, Fax</td>
</tr>
</tbody>
</table>
### Table 6: Tools Used for Testing

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

<table>
<thead>
<tr>
<th>Model</th>
<th>Firmware Version</th>
<th>CPU / OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AltaLink™ C8130 / C8135 C8145 / C8155 / C8170</td>
<td>111.011.000.27020</td>
<td>Intel Atom E3950 (Goldmont)</td>
</tr>
<tr>
<td>AltaLink™ B8145 / B8155/ B8170</td>
<td>111.013.000.27020</td>
<td>Wind River Linux 9.0</td>
</tr>
</tbody>
</table>

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 HDD 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 HDD 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
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.

11.8. Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1R5. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1R5.

Lightship Security, Inc. has determined that the product meets the security criteria in the Security Target, which specifies conformance to the Protection Profile for Hardcopy Devices, Version 1.0, 10 September 2015 and Protection Profile for Hardcopy Devices, Version 1.0 Errata #1. A team of validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation effort was finished August 2021.

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 HDD, dated August 2021, Version 0.8
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

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

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 HDD, v0.8
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 HDD 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 HDD Assurance Activity Report, v0.4