Certification Report

Xerox WorkCentre 3655 and WorkCentre 6655

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-299-CR
Version: 1.0
Date: 30 April 2015
Pagination: i to iii, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CSC Security Testing/Certification Laboratories.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 30 April 2015, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

TABLE OF CONTENTS

Executive Summary

Xerox WorkCentre 3655 and WorkCentre 6655, from Xerox Corporation, is the Target of Evaluation. The results of this evaluation demonstrate that Xerox WorkCentre 3655 and WorkCentre 6655 meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

Xerox WorkCentre 3655 and WorkCentre 6655 are multi-function devices that copy and print with scan and fax capabilities. The Xerox embedded fax component provides local analog fax capability over public switched telephone network connections and also enables LanFax[1]. Xerox's workflow scanning component allows documents to be scanned at the device with the resulting image being sent via email, transferred to a remote file repository, kept in a private (scan) mailbox or placed on a personal Universal Serial Bus (USB) storage device.

CSC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed on 30 April 2015 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Xerox WorkCentre 3655 and WorkCentre 6655, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the CCS Certification Body, declares that the Xerox WorkCentre 3655 and WorkCentre 6655 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] LanFax enables fax jobs to be submitted from the desktop via printing protocols.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is Xerox WorkCentre 3655 and WorkCentre 6655, from Xerox Corporation.

2 TOE Description

Xerox WorkCentre 3655 and WorkCentre 6655 are multi-function devices that copy and print with scan and fax capabilities. The Xerox embedded fax component provides local analog fax capability over public switched telephone network connections and also enables LanFax. Xerox's workflow scanning component allows documents to be scanned at the device with the resulting image being sent via email, transferred to a remote file repository, kept in a private (scan) mailbox or placed on a personal USB storage device.

3 Security Policy

Xerox WorkCentre 3655 and WorkCentre 6655 implement a role-based access control policy to control administrator access to the system. In addition, Xerox WorkCentre 3655 and WorkCentre 6655 implement policies pertaining to the following security functional classes:

- *Security Audit;*
- *Cryptographic Support;*
- *User Data Protection;*
- *Identification and Authentication;*
- *Security Management;*
- *Protection of the TSF;*
- *TOE Access; and*
- *Trusted Path/Channels.*

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate**
Mocana v5.4f	1612
OpenSSL v1.2.3	1051

4 Security Target

The ST associated with this Certification Report is identified below:

Xerox Multi-Function Device Security Target, WorkCentre 3655/6655, Version 1.5, 23 April 2015.

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

Xerox WorkCentre 3655 and WorkCentre 6655 are:

a. EAL 2 augmented, containing all security assurance requirements listed, as well as the following:
    - ALC_FLR.3 Systematic flaw remediation
b. Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
    - FPT_FDI_EXP.1 - Restricted forwarding of data to external interfaces
c. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of Xerox WorkCentre 3655 and WorkCentre 6655 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- *TOE users are aware of the security policies and procedures of their organization, and are trained and competent to follow those policies and procedures.*
- *Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.*
- *Administrators do not use their privileged access rights for malicious purposes.*

6.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- *The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.*

6.3 Clarification of Scope

The FIPS validation for the OpenSSL v1.2.3 module is vendor affirmed and has been ported according to Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program (FIPS IG G.5).

7 Evaluated Configuration

The evaluated configuration for Xerox WorkCentre 3655 and WorkCentre 6655 comprises the following:

Model	**System Software**
WorkCentre 3655	072.060.034.16810
WorkCentre 6655	072.110.044.20510

The publication entitled *Secure Installation and Operation of Your WorkCentre 3655 and WorkCentre 6655* describes the procedures necessary to install and operate Xerox WorkCentre 3655 and WorkCentre 6655 in their evaluated configuration.

8 Documentation

The Xerox Corporation documents provided to the consumer are as follows:

a. Xerox WorkCentre 3655 Multifunction Printer System Administrator Guide v1.0 September 2014;

b. Xerox WorkCentre 3655 Multifunction Printer User Guide v1.0 September 2014;

c. Xerox WorkCentre 6655 Color Multifunction Printer System Administrator Guide v1.0 October 2014;

d. Xerox WorkCentre 6655 Color Multifunction Printer User Guide v1.0 September 2014; and

e. Secure Installation and Operation Of Your WorkCentre 3655 and WorkCentre 6655 v1.2 April 2015.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Xerox WorkCentre 3655 and WorkCentre 6655, including the following areas:

Development: The evaluators analyzed the Xerox WorkCentre 3655 and WorkCentre 6655 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the Xerox WorkCentre 3655 and WorkCentre 6655 security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the Xerox WorkCentre 3655 and WorkCentre 6655 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Xerox WorkCentre 3655 and WorkCentre 6655 configuration management system and associated documentation was performed. The evaluators found that the Xerox WorkCentre 3655 and WorkCentre 6655 configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Xerox WorkCentre 3655 and WorkCentre 6655 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Xerox WorkCentre 3655 and WorkCentre 6655. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Account Creation: The objective of this test goal is to verify the ability to create a local unprivileged user account and a system administrator account with administrator privileges and required password security parameters;

c. User Login: The objective of this test goal is to verify that an unprivileged user must present a valid username and password to authenticate to the Local User Interface (LUI) and WebUI;

d. System Administrator Login: The objective of this test goal is to verify that an administrator must present a valid username and password to authenticate to the LUI and WebUI;

e. Software Self-Test: The objective of this test goal is to verify that a software verification self-test can be initiated and an associated audit log record is generated;

f. Secure Print: The objective of this test goal is to verify that only the user who submitted a secure print job will be able to access the data;

g. IPSec LanFax and IPSec Workflow Scanning: The objective of this test goal is to verify confidentiality through encryption over IPSec;

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

h. Role Based Access Control Policy: The objective of this test case to verify that the TOE implements a role-based access control policy to control administrative access to the system;

i. Audit Download & Verify: The objective of this test goal is to verify that the TOE logs audit events;

j. Verify Immediate Image Overwrite: The objective of this test goal is to verify that a submitted job has been properly overwritten; and

k. SSL Verification: The objective of this test goal is to verify the version of OpenSSL used by the TOE.

10.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;

b. Authentication Bypass: The objective of this test goal is to verify that secure print jobs are discarded if submitted by an unauthenticated user;

c. Session Management: The objective of this test goal is to attempt to perform a session hijack;

d. WebUI and LUI Fuzzing: The objective of this test goal is to subject the WebUI and LUI interfaces to unexpected input;

e. LUI Discovery: The objective of this test goal is to determine whether the LUI is susceptible to reflective cross site scripting or other web application vulnerabilities;

f. Illicit Software Update: The objective of this test goal is to attempt to load an invalid software package via the USB and Line Printer Requester; and

g. PostScript Hack: The objective of this test goal is to attempt to access operating system commands using PostScript.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

10.4 Conduct of Testing

Xerox WorkCentre 3655 and WorkCentre 6655 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test Facility. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that Xerox WorkCentre 3655 and WorkCentre 6655 behave as specified in the ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LUI	Local User Interface
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
USB	Universal Serial Bus

13 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, April 25, 2014.

e. Xerox Multi-Function Device Security Target, WorkCentre 3655/6655, Version 1.5, 23 April 2015.

f. Evaluation Technical Report Xerox Corporation WorkCentre 3655/6655 EAL2+, Version 1.0, 30 April 2015.