Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

Citrix Virtual Apps and Desktops 7 1912 LTSR Premium Edition

26 October 2020

507 LSS 2019

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report has been evaluated at an approved evaluation facility established under the Canadian Centre for Cyber Security (CCCS). 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 Canadian CC Scheme, 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 Canadian Centre for Cyber Security, 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 Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the 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.

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The Citrix Virtual Apps and Desktops 7 1912 LTSR Premium Edition (hereafter referred to as the Target of Evaluation, or TOE), from Citrix Systems, Inc. , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

Lightship Security is the CCEF that conducted the evaluation. This evaluation was completed on 26 October 2020 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, 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.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian CC Scheme and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Citrix Virtual Apps and Desktops 7 1912 LTSR Premium Edition
Developer	Citrix Systems, Inc.

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

EAL 2 + ALC_FLR.2

1.2 TOE DESCRIPTION

The TOE is a desktop and application virtualization software solution that gives organizations control of virtual machines, applications, licensing, and security, while providing anywhere access for any device.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

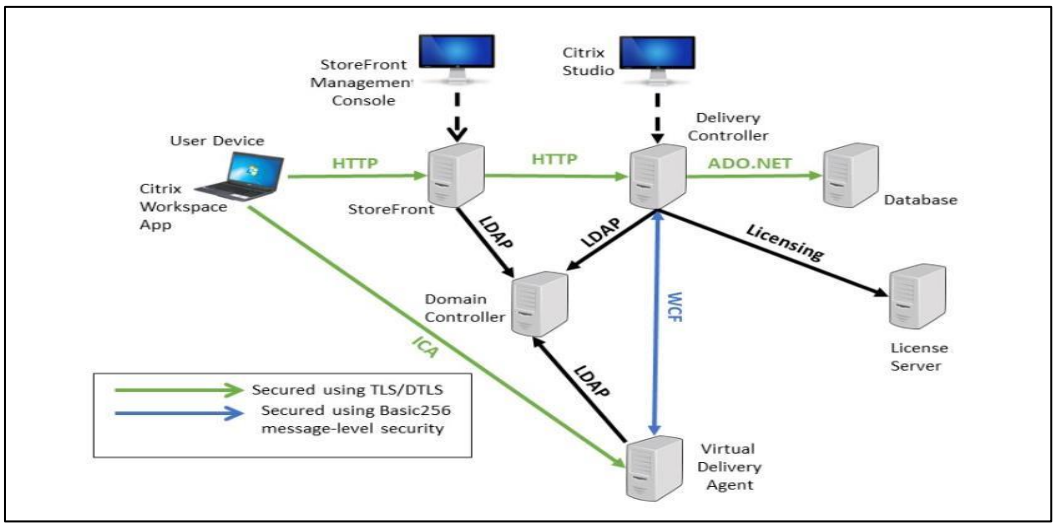

Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE 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.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE servers are installed in a physically secure location that can only be accessed by authorised administrators.
- The Endpoint operating system is securely configured, including appropriate file protection. In particular, a non-administrative user should not have access to facilities to edit the User Device registry.
- Data (including keys) generated, processed, and stored outside the TOE is managed in accordance with the level of risk. This includes the application of appropriate controls to prevent the use of cameras and smart phones to photograph screens and disabling screen capture and print screen functions on endpoints if required by the TOE customer.
- The VM Host software provides virtual machine isolation and is operating correctly and securely.
- Trusted third-party software is operating correctly and securely.

3.2 CLARIFICATION OF SCOPE

Communication between TOE components is protected by Windows cryptographic modules in the operational environment.

The following features/components have not been evaluated and are not to be used in the evaluated configuration:

- Citrix Gateway,
- Citrix Provisioning Services,
- Citrix Profile Management,
- Citrix SD-WAN,
- Citrix Desktop Director,
- Citrix Endpoint Management,
- Application delivery methods other than Citrix Endpoint Management published apps, also known as server-based hosted applications,
- Desktop delivery methods other than VDI desktops,
- Desktop delivery groups of the random type,
- The capability for users to belong to multiple desktop delivery groups,
- The capability for desktop users to be assigned multiple desktops in a desktop delivery group,

- The capability for users to belong to multiple application delivery groups,
- Delegated administrator roles other than full administrators,
- Control of local peripheral support using individual and group policy (only global policy is used),
- The ability for administrators to automatically create virtual desktops and servers using Machine Creation Services,
- Power management of virtual machines via the Delivery Controller,
- The use of multiple Delivery Controllers,
- Connection leasing and use of Zones with Local Host Cache,
- Disconnected sessions,
- Non-brokered sessions,
- Streaming applications using AppV,
- The ability for administrators to deploy Personal vDisks for users and deliver applications using AppV and AppDisks,
- The ability for users to access their personal office PC remotely from Citrix Receiver using the Remote PC Access feature,
- The recording, archiving and playback of the on-screen activity of a user session hosted on a Server or Desktop VDA using the Session Recording feature, and
- Use of the Federated Authentication Service to support SAML-based logon to StoreFront, and the use of unauthenticated (anonymous) delivery groups and StoreFront stores.

4 EVALUATED CONFIGURATION

The evaluated configuration of the TOE comprises the following Citrix Virtual Apps and Desktops 7 1912 LTSR Premium Edition server, build 1912.0.0.24265, and software components running on Windows Server 2019 Standard Edition:

- Delivery Controller build 1912.0.0.24265.
- Studio build 1912.0.0.24265.
- StoreFront (includes the StoreFront Management Console) build 1912.0.0.40.
- Virtual Delivery Agent build 1912.0.0.24265.
- Citrix Workspace app build 19.11.0.50 for Windows.

The TOE requires the following components in the operational environment:

- Citrix License Licensing 11.16.3.
- Microsoft SQL Server 2017.
- Microsoft Active Directory Server in Windows Server 2016 native mode.
- A compatible hypervisor.

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) Common Criteria Evaluated Configuration Guide for Citrix Virtual Apps and Desktops 7 1912 LTSR Premium Edition [CCECG], v01, 2020-10-08 https://www.citrix.com/about/legal/security-compliance/common-criteria.html.

b) Citrix Virtual Apps and Desktops 7 1912 LTSR Premium Edition, Citrix Product Documentation, 5 June 2020 https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/1912-ltsr/citrix-virtual-apps-anddesktops-7-1912-ltsr.pdf.

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE 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.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE 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 the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

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

6.1 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 Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 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. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests;

b. User Authentication: The evaluator verified the TOE supports Usernames/Passwords and smartcards for authentication;

c. Smartcard Authentication Error Conditions: The evaluator verified that various error conditions for smartcard authentication were generated;

d. Configuring StoreFront authentication methods: The evaluator verified that authentication methods for StoreFront can be configured using the Citrix StoreFront administration console;

e. User desktop or apps access: The evaluator verified that a user cannot access a desktop or app when the datastore is not available;

f. User access to delivery groups: The evaluator verified user access to delivery groups;

g. Interrupted network error: The evaluator verified that a network communication failed error message is displayed when a network cable is unplugged from the user device;

h. Breaking out of Applications: The evaluator verified that users are prevented from "breaking out" of published applications;

i. USB preferences: The evaluator verified that USB preferences are available;

j. Administrator control of the USB virtual channel: The evaluator verified that the administrator can control the USB virtual channel;

k. Administrator Control: The evaluator verified that Administrators can control the USB and CDM virtual channels.

6.3.1 FUNCTIONAL TEST RESULTS

The developer's tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 INDEPENDENT PENETRATION TESTING

The penetration testing effort focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their penetration testing effort.

6.4.1 PENETRATION TEST RESULTS

Type 1 & 2 searches were conducted on 8/25/2020 and included the following search terms:

- Citrix Delivery controller and Citrix Studio (1912.0.0.24265)
- Citrix StoreFront (1912.0.0.40)
- Citrix VDA (1912.0.0.24265)
- Citrix License server
- Citrix Desktop Lock (19.12.0.119 Type)
- Citrix workspace 1911 (19.11.0.50)

Vulnerability searches were conducted using the following sources:

- Citrix Support Knowledge Center https://support.citrix.com/search/

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
    - Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
    - US-CERT: http://www.kb.cert.org/vuls/html/search.
- Community (Symantec) security community: https://www.securityfocus.com/
- Tenable Network Security http://nessus.org/plugins/index.php?view=search
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities
- OpenSSL Vulnerabilities: https://www.openssl.org/news/vulnerabilities.html
- Google

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

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

The Information Technology (IT) product identified in this certification report has been evaluated at an approved evaluation facility established under the Canadian Centre for Cyber Security (CCCS). This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CCCS or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 RECOMMENDATIONS/COMMENTS

- It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.
- The evaluator noted that the setup of the TOE requires extensive knowledge of Microsoft Windows services and functionality. It is recommended that customers looking to deploy the TOE have in depth experience with Active Directory and Windows Server.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CCCS	Canadian Centre for Cyber Security
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Citrix Virtual Apps and Desktops 7 1912 LTSR Premium Edition, Security Target, Version 1.1, 26 October 2020.
Evaluation Technical Report, Version 0.9, 26 October 2020.