Communications Security Establishment
Centre de la sécurité des télécommunications

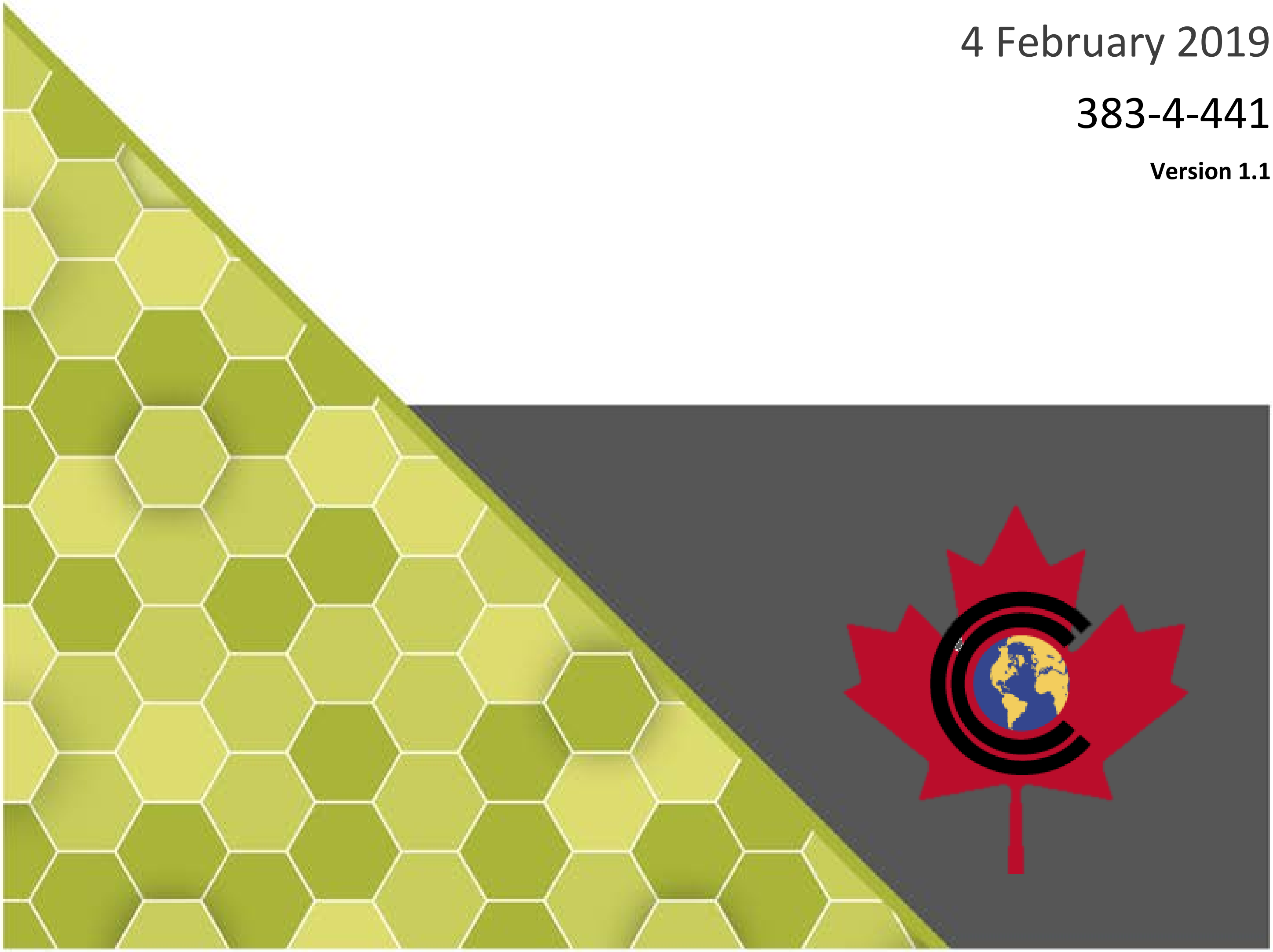
COMMON CRITERIA CERTIFICATION REPORT

VMware Horizon 7 v7.3.3, Horizon Client for Windows v4.6.1 and UAG v3.1.1

4 February 2019

383-4-441

Version 1.1



Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

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 Scheme – 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. 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 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.

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

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

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 Communications Security Establishment.

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 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).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

VMware Horizon 7 v7.3.3, Horizon Client for Windows v4.6.1 and UAG v3.1.1 (hereafter referred to as the Target of Evaluation, or TOE), from VMware, 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 TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed 4 February 2019 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 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.

Communications Security Establishment, as the Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Canadian Certified Products list (CPL) 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	VMware Horizon 7 v7.3.3, Horizon Client for Windows v4.6.1 and UAG v3.1.1
Developer	VMware, Inc.
Conformance Claim	EAL 2+ (ALC_FLR.2)

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.

1.2 TOE DESCRIPTION

The TOE delivers virtual desktops and applications that run in a data center to remote users, allowing them to securely access their desktops and applications from any number of devices either within the enterprise or elsewhere. The TOE does not perform the virtualization itself but rather manages large numbers of desktops and applications. A single administration console provides granular levels of control, allowing customization of the end-user experience, access, and personalization to support corporate policy, along with centralized control, efficiency, and security by having desktop data reside within the data center.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

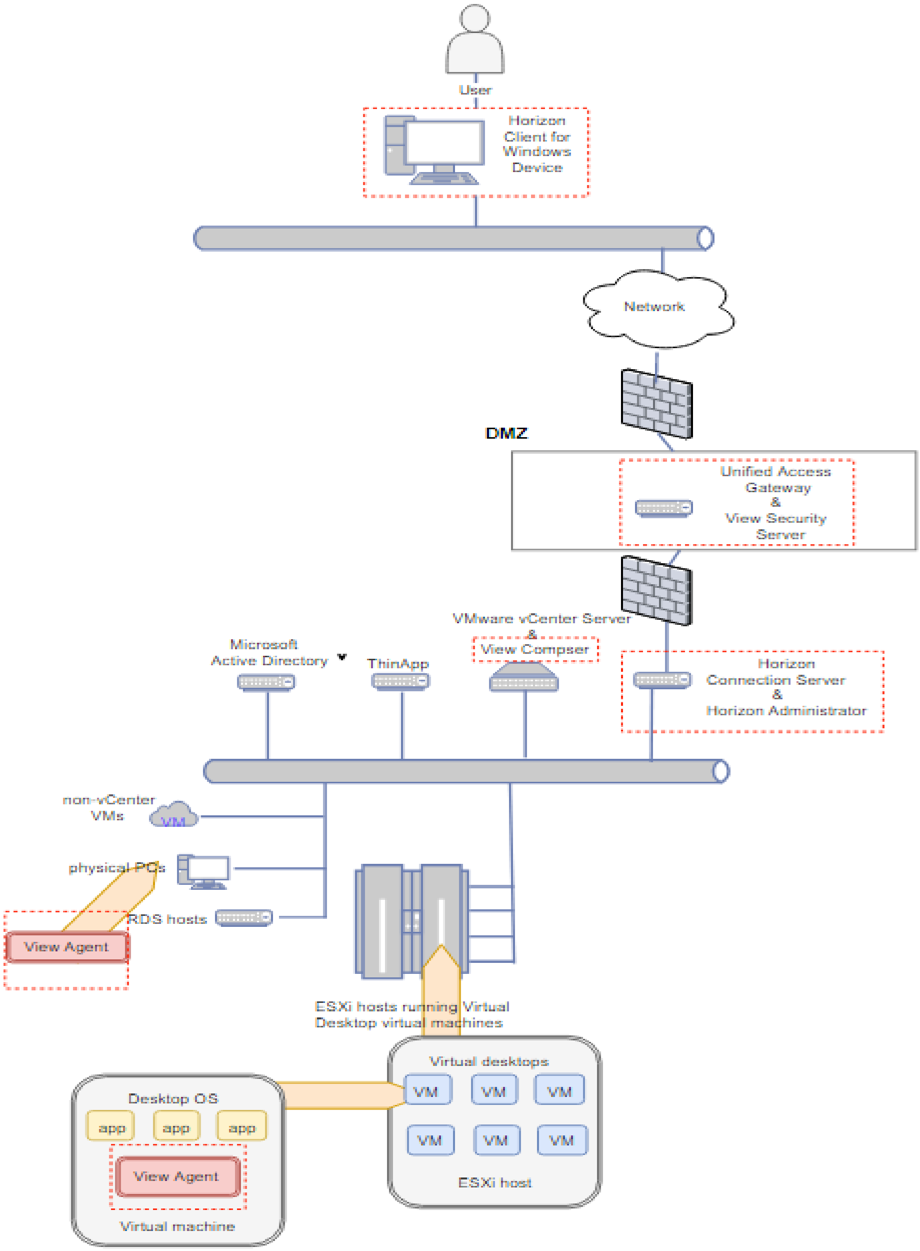

User
Horizon Client for Windows Device
Network
DMZ
Unified Access Gateway & View Security Server
VMware vCenter Server & View Compser
Microsoft Active Directory
ThinApp
Horizon Connection Server & Horizon Administrator
non-vCenter VMs
VM
physical PCs
RDS hosts
View Agent
ESXi hosts running Virtual Desktop virtual machines
Virtual desktops
VM
VM
VM
VM
VM
VM
ESXi host
Desktop OS
app
app
app
View Agent
Virtual machine

Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Session Locking and Termination

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

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic modules were evaluated by the CMVP and are used by the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
OpenSSL FIPS Object Module	2839
Legion of the Bouncy Castle Inc.	2768
VMware Java JCE (Java Cryptographic Extension) Module	2866
Microsoft Corporation Crytptographic Primitives Library	3095
Microsoft Corporation Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 10, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Enterprise LTSB, Windows 10 Mobile, Windows Server 2016 Standard, Windows Server 2016 Datacenter, Windows Storage Server 2016	2937
Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Microsoft Windows 8.1 Enterprise, Windows Server 2012 R2, Windows Storage Server 2012 R2, Surface Pro 3, Surface Pro 2, Surface Pro, Surface 2, Surface, Windows RT 8.1, Windows Phone 8.1, Windows Embedded 8.1 Industry Enterprise, StorSimple 8000 Series, Azure StorSimple Virtual Array Windows Server 2012 R2	2357

3 ASSUMPTIONS AND CLARIFICATIONS 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:

- Appropriate physical security is provided within the domain for the value of the IT assets protected by the TSF and the value of the stored and processed information.
- The VM host software provides virtual machine isolation and is operating correctly and securely
- Administrators are assumed to have configured IPsec associations between security servers and connection servers such that forwarded requests from client components to connection servers, and responses to such requests, are confidentiality and integrity protected.

3.2 CLARIFICATION OF SCOPE

The TOE relies on the underlying Windows operating system for some cryptographic operations. It is important that only those operating systems listed in the evaluated configuration are used.

CMVP certificate #2357 is in a historical state in accordance with SP800-131A Revision 1 Transition (AES/TDES key wrapping. The key wrapping operation is not used by the TOE, as such having the CMVP certificate in historical status will have no impact to the TOE.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

- Horizon Client for Windows v4.6.1 running on Windows 10,
- Horizon Connection Server v7.3.3 running on Windows Server 2016,
- Security Server v7.3.3 running on Windows Server 2016,
- UAG v3.1.1 (FIPS) running on Windows Server 2016,
- View Composer v7.3.3 running on Windows Server 2016,
- Horizon Agent v7.3.3 running on Windows 10 and Winders Server 2012.

4.1 DOCUMENTATION

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

a. Release Notes for VMware Horizon 7 version 7.3.3 Released October 4, 2018

b. VMware Horizon 7 Version 7.3 View Installation Released November 2017

c. VMware Horizon 7 Version 7.3 View Upgrades Released November 2017

d. VMware Horizon 7 Version 7.3 Security Guide Released November 2017

e. VMware Horizon 7 Version 7.3 View Architecture Planning Released November 2017

f. VMware Horizon 7 Version 7.3 View Administration Released November 2017

g. VMware Horizon Client for Windows 4.6.1 Released October 2017

h. Unified Access Gateway Version 3.1 Released October 2017

i. Operational User Guidance and Preparative Procedures for VMware Horizon 7 v7.3.3 Released December 2018

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 (SFRs). 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 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 developers tests;

b. PIV Card Authentication: The objective of this test case is to verify successful and unsuccessful PIV card authentication attempts;

c. Smartcard Authentication: The objective of this test case it to verify successful and unsuccessful smartcard authentication attempts;

d. CAC Card Authentication: The objective of this test case is to verify successful and unsuccessful CAC card authentication attempts;

e. View Agent (OS): The objective of this test case is to verify that the desktop running the View Agent will not be accessible when the Agent and Guest OS are not running or not available;

f. View Agent (Applications): The objective of this test case is to verify that the application running the agent will not be accessible when the application is not published;

g. Verification of Cryptographic Modules: The objective of this test case is to verify the OpenSSL and Bouncy Castle versions on each TOE component; and

h. Security Server: The objective of this test case is to verify that the Security Server is accessible over the Horizon Client and Horizon HTML interfaces and that the Security Server can provide access to allowed resources.

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

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 such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST; and

b. CVE-2018-6971 Test: The objective of this test is to determine whether the TOE is vulnerable to a local information disclosure vulnerability, where an administrator’s password gets written to a log file;

c. CVE-2017-4948 Test: The objective of this test is to determine whether the TOE is vulnerable to out-of-bounds memory read error in Cortado ThinPrint ('TPView.dll'); and

d. CVE-2018-6970 Test: The objective of this test is to verify that the TOE is not susceptible to an out-of-bounds read vulnerability in the Message Framework library. Successfully exploiting this issue may allow a less-privileged user to leak information from a privileged process running on a system where Horizon Connection Server, Horizon Agent or Horizon Client are installed.

6.4.1 PENETRATION TEST RESULTS

The independent penetration testing did not uncover any 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 IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

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 CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE 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.

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
CVE	Common Vulnerabilities Exposure
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
OS	Operating System
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.
VMware Horizon 7 v7.3.3 Security Target, Version 1.1, February 1, 2019.
VMware Horizon 7 v7.3.3 Evaluation Technical Report, Version 0.5, February 4, 2019.