National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

VMware Workspace ONE Boxer Email Client Version 21.05

Report Number: CCEVS-VR-VID11157-2021
Version 1.0
October 05, 2021

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 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Linda Morrison
Clare Parran
Ted Farnsworth

The MITRE Corporation

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of VMware Workspace ONE Boxer Email Client Version 21.05. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Laurel, Maryland, United States of America, and was completed in October 2021. The information in this report is largely derived from the evaluation sensitive Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended and meets the assurance requirements set forth in the *Protection Profile for Application Software Version 1.3* (APP_PP), March 1, 2019, and *Application Software Extended Package for Email Clients v2.0* (EC_EP) June 18, 2015.

The TOE is the VMware Workspace ONE Boxer Email Client Version 21.05 application which is an enterprise email client for iOS and Android mobile devices. The Boxer application provides S/MIME email services and containerizes enterprise data from personal data that resides on the user's mobile device.

In the evaluated configuration, the TOE is installed on a mobile device running iOS 13 (VID11036) as well as a mobile device host running Android 10 (VID11042). The mobile devices must be enrolled and managed by the VMware Workspace ONE Unified Endpoint Management (UEM) at the device level. When the TOE application is installed on the mobile device it is then enrolled as a managed application in UEM in order to obtain its configuration information.

Additionally, the TOE is configured to use ActiveSync to communicate with the Microsoft Exchange server over a TLS v1.2 trusted channel. The Exchange server resides in the operational environment and is for sending and receiving enterprise data such as email, calendar information and appointment data. Whether installed on an Android or iOS device, the application validates the certificates using OCSP. The OCSP responder is also considered part of the operational environment.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5), as interpreted by the Assurance Activities contained in the APP_PP and EC_EP. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units of the ETR for the APP_PP and EC_EP Assurance Activities. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions

justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology 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 Product Compliant List.

Table 1 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.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	VMware Workspace ONE Boxer Email Client Version 21.05
Protection Profile	Protection Profile for Application Software Version 1.3 [APP_PP], Application Software Extended Package for Email Clients v2.0 [EC_EP], and all applicable NIAP Technical Decisions and Policy Letters
Security Target	VMware Workspace ONE Boxer Email Client Version 21.05 Security Target V1.5, dated September 21, 2021
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "VMware Workspace ONE Boxer Email Client Version 21.05" Evaluation Technical Report v1.0 dated September 21, 2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	VMware
Developer	VMware
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Laurel, Maryland
CCEVS Validators	Paul Bicknell Linda Morrison Clare Parran Ted Farnsworth

Table 1 – Evaluation Identifiers

3. Assumptions and Clarification of Scope

3.1 Assumptions

The assumptions are drawn directly from the APP_PP.

3.2 Threats

The threats are drawn directly from the APP_PP and EC_EP.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional 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 level of assurance for this evaluation is defined within the *Protection Profile for Application Software Version 1.3*, *Application Software Extended Package for Email Clients v2.0*, and all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the APP_PP are claimed by the TOE and documented in the ST.
- This evaluation covers only the specific device model and software version identified in this document, and not any earlier or later versions released or in process.
- Consistent with the expectations of the Protection Profiles, this evaluation did not specifically search for, nor seriously attempt to counter vulnerabilities that were not "obvious" or vulnerabilities to security functionality not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. All other functionality provided by these devices, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, the VMware Workspace ONE Boxer Email Client Version 21.05 support of collecting, indexing, analyzing, and storing endpoint system event data as well as managing host sensors was not assessed as part of this evaluation. Further information of excluded functionality can be found in Section 2.3 of the Security Target.

4. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Introduction

TOE type is Application Software Email Client.

The Application Software Email Client TOE type is justified because the TOE is application software that is installed on mobile devices which provides email client services that allows the user to receive, send, manage, and access enterprise email on their mobile device.

4.2 Physical Boundary

VMware Workspace ONE Boxer Email Client Version 21.05 is a software-only TOE. All hardware that is present is part of the TOE's Operational Environment.

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

Component	Description
OCSP Responder	A server deployed within the Operational Environment which confirms the validity and revocation status of certificates.
VMware Workspace ONE Unified Endpoint Management (UEM) Server	The VMware Workspace ONE UEM server is used to manage the VMware Boxer app (TOE) and its host mobile device. The UEM Server provides administrative access through its UEM Console.
Microsoft Exchange Server 2019	Exchange server for sending and receiving emails to and from the Operational Environment configured to use ActiveSync to communicate.
Mobile Device	The hardware that runs the OS in which the application is installed on. The TOE was installed on a certified iOS 13 (VID11036) device and certified Android 10 (VID11042) device. For testing, this evaluation used a Samsung Galaxy S10+ (Android) and on an iPhone Xs (Apple).

Table 2 – IT Environment Components

5. Security Policy

5.1 Cryptographic Support

Depending on which OS the application is installed on, the TOE either invokes the underlying platform or implements its own cryptographic module to perform cryptographic services. All cryptographic mechanisms, whether platform or application provided, use DRBG functionality to support cryptographic operations. Cryptographic functionality includes encryption/decryption services, credential/key storage, key establishment, key destruction, hashing services, signature

services, key-hashed message authentication, and key chaining using a password-based derivation function.

Cryptographic services for the application's S/MIME functionality and TLS communications are provided by the underlying platform when the application is installed on a device running iOS. When installed on a device running the Android OS, the TOE invokes the underlying platform cryptographic libraries for TLS communications and implements an OpenSSL cryptographic module to perform the cryptographic functionality required to support S/MIME (CAVP certificate #A1297).

5.2 User Data Protection

The TOE uses S/MIME to digitally sign, verify, decrypt, and encrypt email messages. The TOE stores all application data in an encrypted Boxer database which is created on the mobile device during installation. The TOE requires that the host platform have full disk encryption enabled to securely store the data. The TOE restricts its network access and provides user awareness when it attempts to access hardware resources and sensitive data stored on the host platform. The TOE displays notification icons that show S/MIME status. Each status is shown as a different color so that the user can quickly identify any issues.

5.3 Identification and Authentication

The TOE relies on the OS to validate X.509.3 certificates for TLS communication. The TOE validates X.509v3 certificates for signing and encrypting emails for S/MIME.

5.4 Security Management

The TOE enforces the application's enterprise policy set by the UEM administrator pushed out to the managed TOE device. The TOE does not use default passwords, and automatically installs and configures the application to protect itself and its data from unauthorized access while also implementing the recommended platform security mechanisms. Changing one's own password from the application is the only management function that can be performed by the owner/user of the mobile device with the TOE installed.

5.5 Privacy

The TOE does not transmit any personally identifiable information (PII) over the network unless voluntarily sent via free text email.

5.6 Protection of the TSF

The TOE does not support the installation of trusted or untrusted add-ons. The user is able to navigate the platform to check the version of the TOE and also check for updates to the application. All updates come from the Google Play Store (Android) or Apple App Store (iOS). The digital signature of the updates is verified by the mobile device platform prior to being installed. The TOE does not replace or modify its own binaries without user interaction. The TOE implements anti-exploitation features, such as stack-based overflow protection, is compatible with security features provided by the OS, and will only use documented APIs and libraries.

5.7 Trusted Path/Channels

The TOE invokes the platform to provide the trusted communication channel between the TOE and the Exchange server. Communications are protected with TLS v1.2. Communication to the Exchange server uses ActiveSync to send and receive emails.

6. Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- VMware Workspace ONE Boxer Email Client Version 21.05 Supplemental Administrative Guidance for Common Criteria – v1.0, September 21, 2021

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

7. Evaluated Configuration

The following table describes the TOE components in the evaluated configuration:

Component	Definition
VMware Workspace ONE Boxer Email Client v 21.05 Application for Apple iOS 13*	VMware Email Client Application
VMware Workspace ONE Boxer Email Client v 21.05 Application for Android 10.0*	VMware Email Client Application

Table 3 - Evaluated Components of the TOE

*certified iOS 13 (VID11036) and certified Android 10 (VID11042).

In its evaluated configuration, the TOE is configured to communicate with the following environment components:

- OCSP Responder
- VMware Workspace ONE Unified Endpoint Management (UEM) Server
- Microsoft Exchange Server 2019
- Mobile Device

To use the product in the evaluated configuration, the product must be configured as specified in the *VMware Workspace ONE Boxer Email Client Version 21.05 Supplemental Administrative Guidance for Common Criteria – v1.0, September 21, 2021* document.

8. IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Assurance Activity Report for a Target of Evaluation "VMware Workspace ONE Boxer Email Client Version 21.05" Assurance Activities Report v1.0, September 21, 2021*.

8.1 Developer Testing

No evidence of developer testing is required in the Evaluation Activities for this product.

8.2 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the APP_PP and EC_EP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that:

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.3 Evaluation Team Vulnerability Testing

The evaluation team reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with the APP_PP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Keyword	Description
Boxer	This is a generic term for searching for known vulnerabilities for the specific product.
ActiveSync	This is a generic term for searching for known vulnerabilities for the network protocol used by the TOE.
OpenSSL Android: (version 1.0.2x)	This is a generic term for searching for known vulnerabilities for the cryptographic library used by the TOE application.
WebView	This is a generic term for searching for known vulnerabilities for the email document (rich text/HTML) viewer used by the TOE application (Android).
Polaris Office (version 4.5.2.0)	This is a generic term for searching for known vulnerabilities for the email attachment viewer used by the TOE application (Android).
WKWebView	This is a generic term for searching for known vulnerabilities for the email document (HTML) and attachment viewer used by the TOE application (iOS).

Table 4 - Keyword Vulnerability Analysis

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources (updated September 20, 2021). The following public vulnerability sources were searched:

- Common Vulnerabilities and Exposures: https://www.cvedetails.com/vulnerability-search.php
- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- US-CERT: http://www.kb.cert.org/vuls/html/search
- SecurITeam Exploit Search: www.securiteam.com
- 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
- Tenable Network Security http://nessus.org/plugins/index.php?view=search

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration. Testing that was conducted under the functional testing that would have been duplication of a vulnerability tests were not re-run. This left one remaining exploit to further explore: malicious binary.

Malicious Binary Analysis

This test analyzes the TOE binary using the most current OSINT threat intelligence data against the TOE Android and iOS package files and verify that they do not contain references to network addresses that are flagged as malicious according to the threat intelligence database.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

9. 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 Evaluation 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. The evaluation determined the TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally, the evaluator performed the Evaluation Activities specified in the APP_PP and EC_EP.

The following evaluation results are extracted from the proprietary Evaluation Technical Report provided by the CCTL and are augmented with the validator's observations thereof.

The Validators reviewed all the work of the evaluation team and agreed with their practices and findings.

9.1 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 VMware Workspace ONE Boxer Email Client Version 21.05 product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the APP_PP and EC_EP in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

9.2 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's TOE Summary Specification. Additionally, the evaluator performed the Evaluation Activities specified in the APP_PP and EC_EP related to the examination of the information contained in the TOE Summary Specification.

9.3 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Evaluation Activities specified in the APP_PP and EC_EP related to the examination of the information contained in the operational guidance documents.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit and the extended assurance requirement ALC_TSU_EXT.1 defined in the APP_PP and EC_EP. The evaluation team found that the TOE was identified and a method of timely updates was described.

9.5 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 APP_PP and EC_EP, and recorded the results in a

Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity Report.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and validated that the vendor fixed all findings with the TOE. The evaluation team also ensured that the specific vulnerabilities defined in the APP_PP and EC_EP were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

9.7 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 test activities 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 performed the Evaluation Activities in the APP_PP and EC_EP, and correctly verified that the product meets the claims in the ST.

10. Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *VMware Workspace ONE Boxer Email Client Version 21.05 Supplemental Administrative Guidance for Common Criteria – v1.0, September 21, 2021* document.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation such as its ability to collect information from its host. All other functionality provided by the product needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11. Annexes

Not applicable

12. Security Target

The security target for this product's evaluation is *VMware Workspace ONE Boxer Email Client Version 21.05 Security Target V1.5*, dated September 21, 2021.

13. List of Acronyms

Acronym	Definition
API	Application Programming Interface
CA	Certificate Authority
CC	Common Criteria
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure over a bidirectional TLS encrypted tunnel
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MAS	Mobile Application Store
MDM	Mobile Device Management
NIAP	National Information Assurance Partnership
OCSP	Online Certificate Status Protocol
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSL	Secure Sockets Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
UEM	Unified Endpoint Management

Table 5 – Acronym Definition

14. Terminology

Term	Definition
Administrator	An individual that has the ability to manage some aspect of mobile device configuration using the VMware Workspace ONE Unified Endpoint Management (UEM) console. UEM is a Mobile Device Management (MDM) product that contains a server and an agent that resides on the mobile device.
Managed Device	Managed devices are those devices that are enrolled and managed by an MDM product. Enrolled devices have an agent installed on the device which provide status and policy information about the device to the UEM. Additionally, the agent is responsible for retrieving configuration information for the managed applications installed on the device.
End User	An individual who possesses a mobile device with the Boxer application installed and enrolled into UEM.

Table 6 - Customer Specific Terminology

Term	Definition
Application (app)	Software that runs on a platform and performs tasks on behalf of the user or owner of the platform, as well as its supporting documentation. The terms *TOE* and *application* are interchangeable in this document.
Application Programming Interface (API)	A specification of routines, data structures, object classes, and variables that allows an application to make use of services provided by another software component, such as a library. APIs are often provided for a set of libraries included with the platform.
Credential	Data that establishes the identity of a user, e.g. a cryptographic key or password.
Developer	An entity that writes application software. For the purposes of this document, vendors and developers are the same.
Operating System (OS)	Software that manages hardware resources and provides services for applications.
Personally Identifiable Information (PII)	Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.
Platform	The environment in which application software runs. The platform can be an operating system, hardware environment, a software based execution environment, or some combination of these. These types platforms may also run atop other platforms.
Security Administrator	An authorized administrator role that is authorized to manage the TOE and its data.

Sensitive Data	Sensitive data may include all user or enterprise data or may be specific application data such as emails, messaging, documents, calendar items, and contacts. Sensitive data must minimally include PII, credentials, and keys. Sensitive data shall be identified in the application's TSS by the ST author.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application an Authorized Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to manage TOE functions or data.
Vendor	An entity that sells application software. For purposes of this document, vendors and developers are the same. Vendors are responsible for maintaining and updating application software.

Table 7 - CC Specific Terminology

15. Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Protection Profile for Application Software Version 1.3.
6. VMware Workspace ONE Boxer Email Client Version 21.05 Security Target v1.5, dated September 21, 2021.
7. VMware Workspace ONE Boxer Email Client Version 21.05 Supplemental Administrative Guidance for Common Criteria – v1.0, September 21, 2021.
8. Assurance Activity Report for a Target of Evaluation "VMware Workspace ONE Boxer Email Client Version 21.05" Assurance Activities Report (AAR) v1.0, dated September 21, 2021.
9. Evaluation Technical Report For a Target of Evaluation "VMware Workspace ONE Boxer Email Client Version 21.05" Evaluation Technical Report (ETR) Version 1.0, dated September 21, 2021