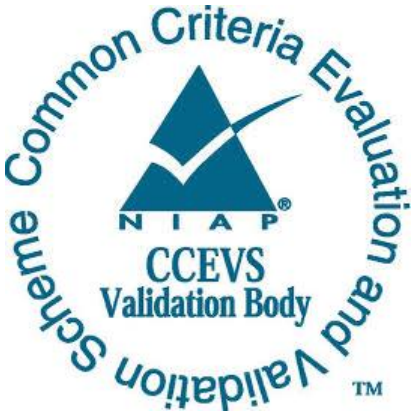
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

IBM MaaS360 v2.91 Cloud Extender

Report Number: CCEVS-VR-10896-2018

Dated: 14 June 2018 Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Acknowledgements

Validation Team

Patrick Mallett, PhD (Lead Validator)

MITRE Corporation
McLean, VA

Jerome Myers, PhD

Aerospace Corporation

Columbia, MD

Common Criteria Testing Laboratory

Brandon Harvey
Trang Huynh
King Ables
Quentin Gouchet
David Rumley

atsec information security corporation

Austin, TX.

Table of Contents

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the IBM MaaS360 v2.91 Cloud Extender solution provided by IBM. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Common Criteria Testing Laboratory (CCTL) atsec information security corporation in Austin, TX, United States of America (NVLAP Lab code 200658) and was completed in June 2018. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CCTL, atsec information security corporation. The evaluation determined that the product is both **Common Criteria (CC) Part 2 Extended and Part 3 Extended** and meets the assurance requirements set forth in the U.S. Government Approved Protection Profile - Protection Profile for Application Software Version 1.2, dated 22th April, 2016.

The TOE consists of the IBM v2.91 Cloud Extender (CE) application. It includes four modules enabling communications functionality with various customer provided services as well as the supporting documentation and a configuration tool. The four modules are:

the following modules:

- Certificate Authority: version 2.93
- Exchange Integration for Managing Active Sync Devices: version 2.3
- Corporate User Visibility: version 2.93
- Corporate Directory Authentication: version 2.93

In addition, the TOE comes with the IBM MaaS360 Cloud Extender configuration tool version 2.93.

The TOE identified in this Validation Report has been evaluated at a NIAP approved CCTL using the "Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4)" (CEM) for conformance to the "Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4)" (CC). 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 (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. 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.

The CCTL, atsec information security corporation, evaluation team concluded that the CC requirements specified by the U.S. Government Approved Protection Profile - Protection Profile for Application Software Version 1.2, dated 22th April, 2016 have been met.

The technical information included in this report was obtained from the IBM MaaS360 v2.91 Cloud Extender Security Target (ST) and analysis performed by the Validation Team.

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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance 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 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 Validated Products List.

Table 1 provides information needed to completely identify the product, including the following.

- 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

Table 1:Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	IBM MaaS360 v2.91 Cloud Extender -- which runs as a service on a Microsoft Windows Server 2012 R2 (x64)

Item	Identifier
PP	U.S. Government Approved Protection Profile - Protection Profile for Application Software Version 1.2, dated 22 April, 2016
ST	IBM MaaS360 v2.91 Cloud Extender Security Target, Version 1.2.2, Date: 2018-05-24
ETR	VID10896 ETR, Version 1.0, date: 2018-04-24
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	IBM Corp.
Developer	IBM Corp.
CCTL	atsec information security corporation, Austin, TX
CCEVS Validators	Jerome Myers, Aerospace Corporation, Columbia, MD Patrick Mallett, MITRE Corporation, McLean, VA

3. Architectural Information

Note that the following architectural description is based on the description presented in the ST.

The TOE consists of the IBM Cloud Extender (CE) application. It includes four modules (listed below) enabling communications functionality with various customer provided services as well as the supporting documentation and a configuration tool.

The application is installed within a MaaS360 customer's own network or DMZ in order to enable services offered by the IBM MaaS360 Enterprise Mobility Management (EMM), a cloud-based multi-tenant platform that provides a mobile device management (MDM) solution.

The Cloud Extender is a Windows service comprised of:

- Core Installer—this functions as a Windows service
- Four CE modules:
    - Certificate Authority: version 2.93
    - Exchange Integration for Managing Active Sync Devices: version 2.93
    - Corporate User Visibility: version 2.93
    - Corporate Directory Authentication: version 2.93

The Cloud Extender consists of multiple processes running simultaneously. It uses the following cryptographic libraries:

- The Windows Cryptography Library API Next Generation (CNG) cryptographic library accessed via the .NET 3.5 framework
- OpenSSL for the IBM MaaS360 Cloud Extender

The Core Installer communicates with the MaaS360 SaaS. It uses Client for URLs (cURL) and Windows crypto for protecting the communications channel between the MaaS360 SaaS application and the Cloud Extender. The Core Installer uses TLS 1.2 and initiates all communication with the MaaS360 SaaS application. Thus, the TOE acts as a TLS client.

The IBM MaaS350 Cloud Extender configuration tool is supplied with the Cloud Extender installation package which can be used during the initial installation as well as on-demand when configuration changes are necessary.

3.1 TOE Evaluated Configuration

The evaluation covers IBM MaaS360 v2.91 Cloud Extender and four modules as detailed in Table 1 below.

The evaluated configuration includes four CE modules, which are packages of scripts and actions that integrate with components of the MaaS360 customer's infrastructure and provides full integration service with that component. Table 2: Description of the Cloud Extender Modules provides descriptions of each of the CE modules.

Table 2: Description of the Cloud Extender Modules

CE Module	Description
Exchange Integration for New Emails Module	The Exchange Integration module interacts with the Exchange Server to automatically discover ActiveSync-connected devices and uploads that device information to the MaaS360® Cloud. The Exchange Integration module automatically quarantines devices, allows only MaaS360 enrolled devices, carries out actions (such as Approve, Block, or Remove device from the Mailbox) sent from MaaS360, and applies ActiveSync device policies. This module supports MS Exchange 2007, 2010, 2013, 2016, Office 365, and Microsoft Business Productivity Online Suite (BPOS)-D.
Corporate Directory Authentication Modules	The User Authentication module interacts with Active Directory and LDAP directories to provide user authentication service for various MaaS360 functions, such as self-service device enrollment with corporate credentials, MaaS360 Portal login, and user management portal. The Cloud Extender supports integration with Lightweight Directory Access Protocol (LDAP) implementations, including

	Active Directory, Domino® LDAP, Oracle® LDAP, Novell® eDirectory LDAP, and OpenLDAP.
Corporate User Visibility Module	The User Visibility module synchs user and group information from LDAP or Active Directory directories to the MaaS360 SaaS application.
Certificate Authority Module	The Certificate Integration module facilitates the automatic provisioning, distribution, and renewal of digital identity certificates to managed mobile devices by using existing Microsoft Certificate Authority (CA), Symantec® CA, or Entrust® Admin Services and Identity Guard. The Cloud Extender interacts with the CA, and then pushes the issued certificates down to enrolled devices by using the following method: It receives certificate requests from the MaaS360 Portal for all enrolled devices that require an identity certificate. It authenticates against the CA or Registration Authority (RA) as a part of the certificate request process. It requests ID certificates by passing the details of the device or user and corresponding attributes as a part of the certificate request. It encrypts the received certificate by using the public key of the requesting device and pushes the encrypted payload to the MaaS360 Portal, which is then delivered to the device. It supports auto-renewals of certificates and makes sure that devices receive the new certificates before the current certificate expires.

3.1.1 Hardware

The hardware platform used during the evaluation was a Dell PowerEdge T110 II with an Intel Core i3 processor.

3.1.2 Operational Environment

The TOE requires the following in its operational environment.

- A configured and operational instance of the MaaS360 SaaS application
- One or more enrolled mobile devices
- A network connection to the MaaS360 SaaS application and the customer's internal network
- A Windows Server 2012 R2 platform on which it runs
- A MS Exchange Server
- An Active Directory Server

- A Network Device Enrollment Server Certificate Authority (NDES CA) server and/or An Entrust Certificate server

3.2 Physical Scope of the TOE

The physical boundary of the TOE consists of the application installer executable and guidance documents. Each of these assets is distributed digitally via the customer's portal.

4. Security Policy

This section summaries the security functionality of the TOE including the following.

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security management
5. Protection of the TOE Security Functionality
6. Timely trusted updates
7. Privacy
8. Trusted path/channels
9.

4.1 Cryptographic Support

The Cloud Extender provides cryptographic support using the Windows platform provided cryptographic services via the Cryptography API: Next Generation (CNG) for the following.

1. TLS connections— TLS connections—CNG is used by Secure Channel (SChannel), enabling the Cloud Extender to communicate with the Exchange Server, Domain Controller, and PKI Certificate Servers using HTTPS, limiting the protocol to TLS 1.2.
2. Protecting data-at-rest using the Encrypted File System (EFS).
3. Encrypting of registry entries using the Data Protection Application Programming Interface (DAPI).

The inclusion of the OpenSSL for the IBM MaaS360 Cloud Extender libraries with the TOE provides cryptographic functionality for the following functions.

1. TLS connections to the MaaS360 Portal and SCEP certificate Servers. (HTTPS using cURL)
2. Encryption of configuration profiles.
3. Device and User Certificate generation for certificate signing requests to a SCEP servers.

4.2 User Data Protection

The application provides user data protection services through restricting access by the application to only those platform-based resources (sensitive data repositories, and network communications) that are needed in order to provide the needed application functionality.

Sensitive application data is encrypted using platform-provided encrypted file system (EFS) services, when stored in non-volatile memory, such as the hard disk drive(s).

4.3 Identification and Authentication

The TOE supports authentication by X.509 certificates by the application and using the platform API.

4.4 Security Management

The Cloud Extender application provides the ability to set various configuration options for the TOE. These options are stored, as recommended by Microsoft, in the Windows Registry and are protected using the Data Protection application programming interface (DPAPI).

During installation, the files installed on the platform are allocated appropriate file-permissions, supporting the protection of the application, and its data from unauthorized access.

4.5 Protection of the TOE Security Functionality

The Cloud Extender application uses only documented Windows APIs. It is packaged with third party libraries which provide supporting functionality

The Cloud Extender application is compiled using stack buffer overrun protection and uses Address Space Layout Randomization (ASLR) techniques.

The Cloud Extender application is packaged and delivered in the Windows Application Software (.EXE) format signed using the Microsoft Authenticode process using the Microsoft Sign Tool.exe (v6.3). It is compiled by IBM with stack-based buffer overflow protection enabled.

4.6 Timely Security Updates

The TOE is not subject to updates. Security updates requires a new version of the TOE to be installed. Installers for the TOE are digitally signed by IBM in accordance to the Microsoft Authenticode process using a Class 3 SHA-256 provided by Symantec.

4.7 Privacy

The Cloud Extender application does not specifically request Personally Identifiable Information (PII).

4.8 Trusted Path/Channels

The Cloud Extender application protects all transmitted data by using TLS 1.2 protected trusted channels.

5. Assumptions and Clarification of Scope

The Security Problem Definition, including the assumptions, may be found in the Protection Profile for Application Software, Version 1.2 and should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the Protection Profile for Application Software, Version 1.2 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 TOE needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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: 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 Protection Profile for Application Software, Version 1.2 and performed by the evaluation team).

The TOE is an example of [USE CASE 3] Communication described in [pp_app_v1.2] as:

"The application allows for communication interactively or non-interactively with other users or applications over a communications channel." The core functionality of the server is outside the scope.

6. Documentation

The following documentation was used as evidence for the evaluation of the IBM MaaS360 v2.91 Cloud Extender.

6.1 Design Documentation

None.

6.2 Guidance Documentation

The following documentation was used as evidence for the evaluation:

- MaaS360 Cloud Extender NIAP Protection Profile Setup and Operations Guide, version 1.12

- Cloud Extender Admin Guide, March 2017.

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when using the products as evaluated.

7. 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, MaaS360 Cloud Extender, Version 2.91, 31 May 2018, Ver 1.1".

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The TOE is composed exclusively of the Cloud Extender application which uses Microsoft Windows Server 2012 R2 as the TOE platform. The TOE environment consists of an additional physical server with various virtual machines. These virtual machines perform services that interface with the Maas360 Cloud Extender Active Directory and Exchange Modules. The NDES certificate module interfaces via HTTPs with the NDES CA over a WAN connection.

The inventory and purpose for each Virtual Machine is as follows:

- 1x VM With Windows Server 2012 R2 acting as a Domain Controller
- 1x VM With Windows Server 2012 R2 to host the Cloud Extender Application (TOE)
- 1x VM With Windows Server 2012 R2 acting as a CA
- 3x VM With Windows Server 2012 R2 acting as intermediary CAs
- 1x VM With Windows Server 2012 R2 acting as a Web Server
- 1x VM With Windows Server 2012 R2 with Exchange Server
- 1x VM with Archlinux and OpenSSL Server and Rocket

All VMs will be joined to a test domain with all of the prerequisites installed and necessary roles and features configured.

Additionally, the Cloud Extender Application is linked to its respective Maas360 cloud portal.

The test requirements defined in the Protection Profile for Application Software, version 1.2 are supplemented with detailed test instructions to ensure a repeatable testing.

7.3 Evaluation Test Tools

The following tools were used by the evaluation team to test the TOE.

- Wireshark network packet analyzer version 1.12.7 with WinPcap version 4.1.3 was used during testing to monitor network traffic, https://www.wireshark.org/ .
- Nmap port scanning tool (version 6.47) was used to scan for open ports on the TOE, https://nmap.org/).
- OpenSSL and the debug utilities s_server and s_client version 1.0.2.k, (https://www.openssl.org/).
- Microsoft Internet Information Services (IIS) within Windows Server 2012 R2 was used as a web server for TLSC and X509 testing.
- Microsoft Standalone SDK version 8.0 (https://developer.microsoft.com/en-us/windows/downloads/windows-8-sdk).
- Sysinternal Suite (https://download.sysinternals.com/files/SysinternalsSuite.zip)
    - procmon version 3.4
    - VMMP version 3.2.1
- Binscope version 2014 (https://www.microsoft.com/en-us/download/details.aspx?id=44995).
- MD5summer version 1.2 (http://www.md5summer.org/).
- Microsoft Enhanced Mitigation Experience Toolkit (EMET) version 5.52 (https://support.microsoft.com/en-us/help/2458544/the-enhanced-mitigation-experience-toolkit).
- Microsoft Windows Server 2012 R2 System Tools:
    - Signtool
    - icacls

8. Evaluated Configuration Setup

The TOE is distributed in a Common Criteria-specific package consisting of ISO files to be installed on vendor hardware platforms. The TOE was installed and configured precisely as specified in the *MaaS360 Cloud Extender NIAP Protection Profile Setup and Operations Guide*. The TOE was in the evaluated configuration at the start of each test.

The TOE was installed within a Microsoft Active Directory Environment within a secure location. External services provided Active Directory, LDAP, NDES CA, Windows Server CA, and Microsoft Exchange in the OE.

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.

All work units defined by the Protection Profile for Application Software received a pass 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 Revision 4 and CEM Version 3.1 Revision 4. The evaluation determined the IBM MaaS360 v2.91 Cloud Extender TOE to be Part 2 extended, Part 3 extended, and to meet the assurance requirements defined by the Protection Profile for Application Software.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied ASE CEM work units and the assurance activities specified in the Protection Profile for Application Software. 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 IBM MaaS360 v2.91 Cloud Extender product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 Protection Profile for Application Software and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development Documentation (ADV)

The evaluation team applied ADV CEM work units. The evaluation team assessed the documentation and found it adequate to aid in understanding how the TSF provides the security functions. The documentation consists of a functional specification contained in the Security Target and guidance documents.

The validation team 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.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied AGD CEM work units and assurance activities specified in the Protection Profile for Application Software. 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. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validation team 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 Protection Profile for Application Software and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied ALC CEM work units and assurance activities specified in the Protection Profile for Application Software. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer is able to identify the evaluated TOE.

The validation team 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 Protection Profile for Application Software and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied ATE CEM work units and assurance activities specified in Protection Profile for Application Software. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. The evaluation team performed devised an independent set of tests as mandated by the protection profile.

The validation team 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 Application Software PP and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied VAN CEM work units and assurance activities specified in the Protection Profile for Application Software, version 1.2. The evaluation team ensured that the TOE does not contain known exploitable flaws or weaknesses based upon the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

The evaluator searched the Common Vulnerabilities and Exposures site (https://cve.mitre.org/cve/cve.html). The search was performed during the period of January 22-26, 2018. The search was repeated on February 20, March 8, March 18, April 9, and April 23. No vulnerabilities applicable to the TOE in the evaluated configuration were found.

The search terms used were determined based on the TOE components and product name.

Keywords used in the searches were: "cloud extender"; "maas"; "sqlite"; "openssl"; "libcurl"; "zlib"; "protobuf"; "boost"; "lua"; "lua curl"; "luasql"; "dotnetzip"; "nsis"; "cmarkup"; "gloox"; "installshield"; "visual C++"; "vc++", "bitwise operation".

The evaluator also searched the vendor support page at;

https://www.ibm.com/support/home/product/R442649B24778J14/IBM_MobileFirst_Protect_(MaaS360).

The validation team 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 Protection Profile for Application Software, version 1.2 and that the conclusion reached by the evaluation team was justified.

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 performance of the testing defined by the Protection Profile for Application Software, version 1.2 and the penetration tests 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 Protection Profile for Application Software, version 1.2 and correctly verified that the product meets the claims in the ST.

10. Validator Comments/Recommendations

It is recommended the administrator exercise caution installing or running other applications on the TOE server that could allow non-administrator access to the system. One of the potential vulnerabilities that was considered is mitigated by an assumption that only administrators can directly access the server. This is a valid assumption as long as no other applications are installed on the server. In the event that a customer desires to permit non-administrators direct access to the server platform on which the TOE resides or to install other applications that could potentially result in non-administrator access then further action should be considered to mitigate the potential vulnerability. The specific threat is associated with an OpenSSL side channel timing attack on RSA key generation, described by CVE-2018-0737. There is a simple source code fix mentioned with the CVE that would completely eliminate this potential attack even if other users could access the server. That fix can be manually applied, but it has not yet been incorporated into a formal patch available through the trusted update process. The vendor plans to release a future version of the TOE that will include an updated version of OpenSSL when the fix is incorporated into the OpenSSL distribution.

11. Annexes

Not applicable.

12. Security Target

IBM MaaS360 v2.91 Cloud Extender Security Target, version 1.2.2, dated 2018-05-24.

13. Glossary

The following definitions are used throughout this document.

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.
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
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.
Feature	Part of a product that is either included with the product or can be ordered separately.
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.
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.

14. Bibliography

The evaluation team used the following documents to produce this Validation Report:

- Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
- U.S. Government Approved Protection Profile - Protection Profile for Application Software Version 1.2, dated 22nd April, 2016.
- IBM MaaS360 v2.91 Cloud Extender Security Target, version 1.2.2, dated 2018-05-24