ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Ivanti EPMM 11.9

Ivanti EPMM 11.9

Maintenance Report Number: CCEVS-VR-VID11196-2023

Date of Activity: 13 July 2023

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016
- Impact Analysis Report for Ivanti EPMM 11.9, version 0.4, 27 June 2023
- MobileIron Core 11.0.0.0 Device Management Guide for Android and Android enterprise Devices, December 3, 2020 was revised to Ivanti EPMM 11.4.0.0 - 11.9.0.0 Device
- Protection Profile for Mobile Device Management, Version 4.0, April 25, 2019
- PP-Module for MDM Agent, Version 1.0, April 25, 2019
- Functional Package for TLS, Version 1.1, March 1, 2019

Original Documentation:

- MobileIron Platform 11 Security Target, Version 0.6, 08/31/2021
- Core and Android and iOS Client Mobile Device Management Protection Profile Guide for Release 11, August 2021
- On-Premise Installation Guide for MobileIron Core and Enterprise Connector 11.0.0.0, December 3, 2020
- Getting Started with MobileIron Core 11.0.0.0, December 3, 2020
- MobileIron Core 11.0.0.0 Device Management Guide for Android and Android enterprise Devices, December 3, 2020
- MobileIron Core 11.0.0.0 Device Management Guide for iOS and macOS Devices, December 3, 2020
- MobileIron Core 11.0.0.0 System Manager Guide, December 3, 2020
- MobileIron Core 11.0.0.0 Apps@Work Guide, November 19, 2020

Revised Documentation:

- Ivanti Endpoint Manager Mobile 11.9 Security Target, Version 0.7, 06/16/2023

- Core and Android and iOS Client Mobile Device Management Protection Profile Guide for Release 11, 2023.
- On-Premise Installation Guide for Ivanti EPMM and Enterprise Connector 11.4.0.0 - 11.9.0.0, February 2023
- Getting Started with Ivanti EPMM 11.4.0.0 - 11.9.0.0, February 2023
- Ivanti EPMM 11.4.0.0 - 11.9.0.0 Device Management Guide for Android and Android Enterprise Devices, February 2023
- Ivanti EPMM 11.4.0.0 - 11.9.0.0 Device Management Guide for iOS and macOS Devices, February 2023
- Ivanti EPMM 11.4.0.0. - 11.9.0.0 System Manager Guide, 2023
- Ivanti EPMM 11.4.0.0 - 11.9.0.0 Apps@Work Guide, February 2023

Assurance Continuity Maintenance Report:

Gossamer submitted an Impact Analysis Report (IAR) for the Ivanti EPMM 11.9 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 6 April 2023. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes.

The evaluation evidence submitted for consideration consists of the Security Target, the Administrator’s Guide, and the Impact Analysis Report (IAR). The ST, Admin Guide, and IAR were updated.

The updated documentation table, the minor change breakdown and the vulnerability analysis have all been pulled directly from the IAR.

Documentation updated:

Original CC Evaluation Evidence	Evidence Change Summary
MobileIron Platform 11 Security Target, Version 0.6, 08/31/2021	Updated to reflect the change in TOE identification/ branding. The ST was also revised to identify that CentOS has been updated to 7.9 (as a result of applying patches).
Design Documentation: See Security Target and Guidance	See Security Target and Guidance changes in this table
Guidance Documentation: • Core and Android and iOS Client Mobile Device Management Protection Profile Guide for Release 11, August 2021 o On-Premise Installation Guide for MobileIron Core and	The guidance documentation has primarily been revised to address the renaming/rebranding of the product from MobileIron Core to Ivanti EPMM. The Core and Android and iOS Client Mobile Device Management Protection Profile Guide

Enterprise Connector 11.0.0.0, December 3, 2020 o Getting Started with MobileIron Core 11.0.0.0, December 3, 2020 o MobileIron Core 11.0.0.0 Device Management Guide for Android and Android enterprise Devices, December 3, 2020 o MobileIron Core 11.0.0.0 Device Management Guide for iOS and macOS Devices, December 3, 2020 o MobileIron Core 11.0.0.0 System Manager Guide, December 3, 2020 o MobileIron Core 11.0.0.0 Apps@Work Guide, November 19, 2020	for Release 11 has been revised to 1) address rebranding, 2) to reflect that some algorithms that needed to be administratively removed are now removed by default, and 3) to add instructions to explain that the new CRL pruning feature should NOT be used in the evaluated configuration. The other guidance documents identified in the Security Target have been revised in minor ways to reflect the incremental changes identified in the release notes and analyzed earlier in this report. Each current document has a “New feature Summary” that identifies the changes that affect that document.
Lifecycle: None	No changes required.
Testing: None	No changes required. Ivanti has performed regression testing on each incremental product release and has generally ensured the security and management functions continue to operate as claimed.
Vulnerability Assessment: None	The public search was performed on 4/4/2023 and repeated on 6/1/2023 and 6/27/2023. No public vulnerabilities exist in the product. See analysis results below, which includes responses from Ivanti on a number of potential issues.

Changes to the TOE:
The changes are summarized below.

Major Changes

None.

Minor Changes

Notable Changes:

There are a relatively small number of updates that are considered more significant that have accumulated across 9 product updates. The change having the most impact on any actual security claim is the addition of a certificate pinning function. While the requirements do not directly address that, there are test cases for that and those test cases were not performed during the evaluation since the function did not yet exist. As such, while this function serves to add security, it should not be considered to be evaluated and this has been explicitly noted in the revised Security Target. The notable changes to the TOE are summarized below:

Feature	Impact Analysis
Certificate pinning to prevent Man-in-the-middle attacks	While this is a new security feature, it only serves to potentially add to and not otherwise impact the claimed and evaluated security function related to TLS X509 requirements. This function is not enabled by default and requires explicit administrator action to enable. Using this new function in addition to the evaluated function does not impact the evaluated function and as such should not be disallowed in an evaluated configuration, although it has not been evaluated or tested by a third party and cannot be claimed as evaluated and caution should be exercised.
Certificate pinning options now available from Certificate Management page	This is the user interface for the preceding function and only serves to present an additional configuration option and as such does not impact any evaluated security claims.
Support for mutual authentication between Core and Sentry	Sentry is an optional, non-evaluated component. As such, adding additional security for its communication channel does not impact any evaluated security claims.
Support for IdP-based device registrations	DEP is an optional enrollment method in the evaluated configuration. This additional feature provides a method to introduce additional information and checks for iOS enrollment via DEP, but does not otherwise affect the enrollment method (that is really controlled by Apple) and does not impact any evaluated security claims.
Export to CSV Installed Apps (App Inventory) Search Results	This is an added feature to export search results in CSV form. This does not impact any evaluated security claims.

Weaker SSH algorithms removed from Core in favor of stronger ones	This change removed by default not-allowed algorithms for SSH, however, SSH was not included in scope of the evaluation and as such this does not impact any evaluated security claims.
New option to upload Certificate Authority chain for SCEP enrollment configurations	The evaluated TOE supports acting as a root CA or an intermediate CA. This change allows an explicit certificate chain to be configured when multiple options are available from a specific SCEP CA. However, device certificates are still issued from the configured CA certificate and the verification of those certificates is unchanged from the evaluation, so this does not impact any evaluated security claims.
Support for Entrust API version 11	Interoperation with Entrust was not a subject of the evaluation and as such this does not impact any evaluated security claims.
Support for bridging old and new client mutual authentication CA certificates	The process of changing a CA certificate was not a subject of the evaluation of the server. As such, this is a new optional feature that is not evaluated and does not have to be used and as such does not impact any evaluated security claims.
Core support for Splunk Heavy Forwarder mutual authentication	Splunk features were not a subject of the evaluation and as such this does not impact any evaluated security claims.
New customization options for the self-service user portal (SSP)	These new settings basically allow an administrator to suppress things on the user pages to customize that portal. This portal was not considered security relevant during the evaluation and is not related to any security claims and as such does not impact any evaluated security claims.
Support for Sentry-to-Core TFE mutual authentication	Sentry is an optional, non-evaluated component. As such, adding additional security for its communication channel does not impact any evaluated security claims.

Administrators can copy existing managed app configuration settings and download updates	This change affects the managed app administrator interface. It provides additional options to copy and edit app configurations, but does not serve to affect any evaluated security claims.
Support for Private DNS	This change serves to provide additional DNS configuration support that is not among the evaluated management claims and as such does not serve to affect any evaluated security claims.
Android File Transfer Configuration	This change serves to provide additional File Transfer support that is not among the evaluated management claims and as such does not serve to affect any evaluated security claims.
Android Bulk Enrollment	Enrollment tokens were not a subject of the evaluation so this change does not impact any evaluated security claims.
Support for pushing OS software to multiple devices	This change allows multiple devices to be selected for updates rather than a single device at a time. The same function is implemented iteratively for all devices and as such this does not affect the underlying evaluated function so this change does not impact any evaluated security claims.
Samsung Firmware E-FOTA decommissioned	This change is related to a feature that was not part of the evaluation and as such does not serve to affect any evaluated security claims.
Samsung Knox Dual Encryption (DualDAR)	This change is related to a feature that was not part of the evaluation and as such does not serve to affect any evaluated security claims.
Ability to set apps to the foreground in devices	This change is related to a feature that was not part of the evaluation and as such does not serve to affect any evaluated security claims.

Android: Support for Common Criteria (CC) mode extended to Android 11+ devices	This change is related to new feature support not originally in the evaluated devices and as such does not serve to affect any evaluated security claims. There was a specific change to add support for a Google API. Note that the evaluation only claims evaluated Samsung devices and iOS devices so this Google API is outside the scope of the evaluation.
End of support for Android 5.0 and Android 5.1	This change is related to devices that predate any claimed in the evaluation and as such does not serve to affect any evaluated security claims.
Google official device admin deprecation	This change is related to a feature that was not part of the evaluation and as such does not serve to affect any evaluated security claims.
Corporate wallpaper for Android devices	This change is related to a feature that was not a subject of the evaluation and as such does not serve to affect any evaluated security claims.
Account-driven Apple User Enrollment	This change is related to an optional enrollment method that was not included in the evaluation and as such does not serve to affect any evaluated security claims.
Unregistered devices can now redirect to Core from Office 365	This change is related to an optional enrollment method that was not addressed in the evaluation and as such does not serve to affect any evaluated security claims.
Enable app restrictions for all supported devices	This change is related to a feature that was not a subject of the evaluation and as such does not serve to affect any evaluated security claims.
Android Enterprise Enable Single App Kiosk added to pin a single app to device screen	This change is related to a feature that was not a subject of the evaluation and as such does not serve to affect any evaluated security claims.
Windows registration configurations enabled upon upgrade	Management of Windows devices was not included in the evaluation and as such this change does not serve to affect any evaluated security claims.

Release Note Changes:
There are a large number of relatively minor updates that have accumulated across 9 product updates. In each case, analysis has concluded that there are no impacts to evaluated security functions. The majority of the changes simply add new features that do not have any impact on any claims. In some cases, possible values or range of values have been changed where the requirements do not dictate specific values. In other cases, changes are related to rebranding or representation of information to users and administrators.

In addition to these changes, Ivanti has also applied patches that have been made available to address bugs identified in its components including patching CentOS. The CentOS version has moved from 7.6 to 7.9 but this is a version change and no functions of the Server have changed as a result. These individual bugs have not been specifically addressed here since none has any direct effect on any security function, but it has been important to address any identified bugs. While not identified, the vulnerability analysis later in this document identifies issues that have been identified and addressed over time.

The algorithm certificates have not changed as the crypto library has not changed. The OS does not perform any cryptographic functions as they are implemented in the TOE. The change between CentOS 7.6 and 7.9 is a minor version change and according to Policy 5 item 4.c.1, this change is permitted.

Regression Testing:
Ivanti has performed regression testing on each incremental product release and has generally ensured the security and management functions continue to operate as claimed.

NIST CAVP Certificates:
No changes to CAVP certificates.

Vulnerability Analysis:
The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 6/27/2023 (from 6/1/2023) with the following search terms: "Endpoint Manager Mobile", "EPMM", "Mobile Iron", "Mobile@work", "Openssl", "Bouncy Castle", "GNU Core Utilities", "Ivanti", "CentOS 7", "CentOS 7.9", "Apache 2.4", "Xeon E5".

The search resulted in no vulnerabilities that are applicable to the TOE. No residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

Conclusion:
The evaluation evidence consists of the Security Target and CC-specific Guidance Documentation. Both the Security Target and Guidance Documentation were revised to reflect the changes in product name/branding and to identify that CentOS has been updated to 7.9 (as a result of applying

patches). Furthermore, the guidance documents have had incremental minor updates to correspond to changes identified in release notes and summarized earlier in this report.

The overall impact is minor. This is based on the rationale that updates do not change any security policies of the TOE and are unrelated from SFR claims. The updates described above were made to support the TOE rebranding and feature updates.

There are no changes to TSF Interfaces, no hardware changes, no SFR changes, no SAR changes, no changes to assumptions threats or objectives, and no new assurance evidence.

Regression testing was done and was considered adequate based on the scale and types of changes made. The vendor also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance.

The TOE now supports certificate pinning, but this functionality is disabled by default and requires administrator configuration to enable it. The ST and other Checkout documents do not make any claims that this functionality is supported.

Therefore, CCEVS agrees that the original assurance is maintained for the product.