ASSURANCE CONTINUITY MAINTENANCE REPORT FOR BlackBerry Unified Endpoint Management (UEM) Server and Android Client

UEM Server and Android Client, version 12

Maintenance Report Number: CCEVS-VR-VID11040-2022

Date of Activity: 27 April 2022

References:

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 2.0, 8 September 2008;
- BlackBerry NIAP Impact Assessment Report, 27 April 2022
- PP-Configuration for Mobile Device Management (MDM) and MDM Agents, Version 1.0, 2020-01-27
- Protection Profile for Mobile Device Management, Version 4.0, 2019-04-25 (MDMPP40)
- PP-Module for MDM Agents, Version 1.0, 2019-04-25 (MDMA10)
- Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019 (PKGTLS11)

Documentation reported as being updated:

- Security Target:
  - BlackBerry Unified Endpoint Management (UEM) Server and Android Client, Version 12 Security Target, Version 0.7, 09 March 2022

- The TOE consists of server and client component for Android iOS devices. The following set of claimed devices is supported by this assurance maintenance.

-

Evaluation Name	Devices
Apple iOS14: iPhones (VID 11146)	iPhone 6s
	iPhone 6s Plus
	iPhone SE
	iPhone 7
	iPhone 7 Plus
	iPhone 8
	iPhone 8 Plus
	iPhone X
	iPhone XS
	iPhone XS Max
	iPhone XR
	iPhone 11
	iPhone 11 Pro
	iPhone 11 Pro Max
	iPhone SE (2nd gen)
	iPhone 12 mini
	iPhone 12
	iPhone 12 Pro
	iPhone 12 Pro Max
Samsung Galaxy Devices Android 11 – Fall (VID 11211)	Galaxy A52 5G
	Galaxy A71 5G
	Galaxy Tab Active3
	Galaxy A42 5G
	Galaxy A51 5G
Samsung Galaxy Devices on Android 11- Spring (VID 11160)	Galaxy S21+ 5G
	Galaxy S21 5G
	Galaxy S21 5G FE
	Galaxy Z Fold3 5G
	Galaxy Z Fold2 5G
	Galaxy Fold 5G
	Galaxy Fold
	Galaxy Z Flip3 5G
	Galaxy Z Flip 5G
	Galaxy Z Flip
	Galaxy Note20 Ultra 5G
	Galaxy Note20 Ultra LTE
	Galaxy Note20 5G
	Galaxy Note20 LTE
	Galaxy S20 Ultra 5G
	Galaxy S20+ LTE
	Galaxy S20 5G
	Galaxy S20 LTE
	Galaxy S20 FE
	Galaxy S20 TE
	Galaxy Tab S7+
	Galaxy Tab S7
	Galaxy Tab S6
	Galaxy A51
	Galaxy Note10+
	Galaxy Note10 5G

	Galaxy Note10+ 5G
	Galaxy Note10
	Galaxy S10+
	Galaxy S10 5G
	Galaxy S10
	Galaxy S10e
Samsung Galaxy Devices on Android 10 – Fall (VID 11109)	Galaxy A71 5G
	Galaxy A51 5G
	Galaxy Tab Active3
	Galaxy Tab S4
Samsung Galaxy Devices on Android 10 – Spring (VID 11042)	Galaxy S20 FE
	Galaxy Fold2
	Galaxy Fold 5G
	Galaxy Fold
	Galaxy Note20+ 5G
	Galaxy Note20+ LTE
	Galaxy Note20 5G
	Galaxy Note20 LTE
	Galaxy Tab S7+
	Galaxy Tab S7
	Galaxy Z Flip 5G
	Galaxy S20 Ultra 5G
	Galaxy S20+ 5G
	Galaxy S20+ LTE
	Galaxy S20 5G
	Galaxy S20 TE
	Galaxy S20 LTE
	Galaxy XCover Pro
	Galaxy A51
	Galaxy Note10+ 5G
	Galaxy Note10+
	Galaxy Note10 5G
	Galaxy Note10
	Galaxy Tab S6 5G
	Galaxy Tab S6
	Galaxy S10 5G
	Galaxy S10+
	Galaxy S10
	Galaxy S10e
	Galaxy Z Flip
	Galaxy Note9
	Galaxy XCover FieldPro
	Galaxy S9+
	Galaxy S9

Assurance Continuity Maintenance Report:

The BlackBerry corporation has prepared and submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 19 April 2022. An 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 2.0.

The purpose of this Assurance Continuity Maintenance Report (ACMR) is to summarize and present the findings of CCEVS' analysis of the IAR and associated evidence submitted in support of the changes to the original evaluation, and to make a determination regarding the appropriateness of Assurance Maintenance Continuity for the evaluation.

Introduction:

The evaluation, VID11040, was conducted by Gossamer Laboratories. The product met the security requirements specified by the NIAP approved protection profiles:

- Protection Profile for Mobile Device Management, Version 4.0, 2019-04-25 (MDMPP40)
- PP-Module for MDM Agents, Version 1.0, 2019-04-25 (MDMA10)

BlackBerry has requested an assurance maintenance activity for the product to update the original evaluation and changes to the original product are detailed in the IAR.

Summary Description:

It is reported that there are no changes to the BlackBerry MDM (Mobile Device Management), TLS (Transport Layer Security) or the BlackBerry Agent. It is also reported that there are no changes to the development environment of the validated TOE.

Reported changes include applying security patches to the TOE. The documentation has been updated to reflect the current software update version, the Security Target, Administration Guide and Planning, Installation and Deployment Guide.

Changes to the TOE Product

TOE Components	Description
TSF Interfaces	There are no claimed changes to the TSF Interface
TSF Platform (Hardware)	There are no claimed changes to the TOE hardware
SFRs	There are no claimed changes to the SFRs

TOE changes to existing functionality:

Feature	Description
N/A	No changes to TOE

New Features:

Feature	Description
Additional functionality was added to support Android Enterprise device logging	This additional functionality is not claimed. This functionality is not enabled and is by default disabled.

The IAR also contains a list of "New features". These features are identified as being non-security features that have no impact on the TSF Interfaces, TOE and SFRs. An impact rationale was provided and identified each new feature as being a minor change. The impact rationale was reviewed, and the majority of the features are outside of the scope of the evaluation, a few were upgrades to support product stability, or address protocols not required by the evaluated products. The listed new features, as described, should be considered to be minor changes.

TOE security patches:
Security patches were applied to the TOE and they are the only reported changes to the TOE. The patches addressed publicly reported vulnerabilities and defects. The updated vulnerability analysis included a description for each security update. The security updates were found to have no impact to the security functionality of the TOE.

Bug Fixes:
A detailed list of Bug Fixes was included in IAR. The fixes cover releases 12.15, 12.14, and 12.13. The bug fixes are claimed to be non-security relevant and do not impact the TOE's security features. The fixes are identified as correcting either operational or functional defects. The descriptions for the fixes were reviewed and the corrections indicate that the fixes are outside of the TOE's security boundary and should be considered minor.

Regression Testing:

Regression testing was performed on the required security patches to ensure that the validated claims continued to be satisfied. All tests were satisfied and passed.

Vulnerability Analysis:

An updated search for vulnerabilities was performed, on the updated TOE, 27 April 2022. The results of the vulnerability assessment were included in the IAR. All new TOE vulnerabilities, version 12.12 or later, were claimed to have been mitigated.

The following search terms were used in the updated vulnerability analysis:

- BlackBerry
- UEM

- TLS
- BlackBerry Client
- Microsoft SQL
- Certicom Security Builder GSE-J Crypto Core 2.9.2
- 12.12 to 12.16

ID	CVE	Resolution	Mitigation
2021-22154	https://nvd.nist.gov/vuln/detail/CVE-2021-22154	https://support.blackberry.com/kb/articleDetail?articleNumber=000078971	Vulnerability mitigated by reducing access to specially crafted links
2021-22153	https://nvd.nist.gov/vuln/detail/CVE-2021-22153	https://support.blackberry.com/kb/articleDetail?articleNumber=000078971	Vulnerability resolved by requiring Admin rights to Console
2021-22152	https://nvd.nist.gov/vuln/detail/CVE-2021-22152	https://support.blackberry.com/kb/articleDetail?articleNumber=000078971	Vulnerability mitigated by requiring Admin privileges
2020-6933	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6933	https://support.blackberry.com/kb/articleDetail?articleNumber=000068112	Workaround in this patch uses a more restrictive pattern matching and replaces the standard java 8 pattern matching

NIST Certificates:
The NIST certificates are not impacted by the assurance maintenance because the same processors and software versions as detailed in the certificates are still used.

Conclusion:

CCEVS reviewed the description of the changes which consisted of the required security patches. There were no changes to the TSF interfaces, SFRs, or security functions introduced by the TOE patches or bug fixes. All of the changes were considered to be minor in impact. In addition, the existing NIST CAVP certifications were also not impacted by any of the changes.

The CCTL also reported that there was only one outstanding vulnerability associated with any of the models. The vendor has proposed a workaround by upgrading to the latest UEM, which includes limiting the java 8 regular expression vulnerability.

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