# ASSURANCE CONTINUITY MAINTENANCE REPORT FOR
# Zebra Devices on Android 13

## Maintenance Update of Zebra Devices on Android 13

**Maintenance Report Number:** CCEVS-VR-VID11486-2025

**Date of Activity**: 25 March 2025

**References:**

- Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0, 12 September 2016.
- Zebra Devices on Android 13 Security Target, Version 0.5, 3/13/2025.
- Impact Analysis Report for Zebra Devices on Android 13, Revision 1.1, 3/13/2025.

## Evaluated TOE

- **CR Title** – Common Criteria Evaluation and Validation Scheme Validation Report Zebra Devices on Android 13
- **Conformance**
    - PP-Configuration for Mobile Device Fundamentals, Bluetooth, and WLAN Clients, Version 1.0, 11 October 2022 (CFG_MDF-BT-WLANC_V1.0)
        - The PP-Configuration includes the following components:
            - Base-PP: Protection Profile for Mobile Device Fundamentals, Version 3.3, 12 September 2022 (PP_MDF_V3.3)
            - PP-Module: PP-Module for Bluetooth, Version 1.0, 15 April 2021 (MOD_BT_V1.0)
            - PP-Module: PP-Module for WLAN Clients, Version 1.0, 31 March 2022 (MOD_WLANC_V1.0)
    - Package Claims:
        - Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 (PKG_TLS_V1.1)
- **CR Report #: CCEVS-VR-VID11486-2024**
- **CR Version** – 1.0
- **CR Date** –August 8, 2024

## Current AM TOE Updated

## Documentation Updated:

| CC Evidence | Evidence Change Summary |
|---|---|
| Zebra Devices on Android 13 Security Target, Version 0.4, 07/26/2024 | Zebra Devices on Android 13 Security Target, Version 0.5, 03/13/2025<br>Updates identify the new product models and ST version number |
| **Guidance Documentation**:<br>Administrator Guidance for Zebra Devices (SD660), Version 0.4, 06/14/2024 | Administrator Guidance for Zebra Devices (SD660), Version 0.4, 06/14/2024. No changes. |
| Administrator Guidance for Zebra Devices (6375), Version 0.4, 06/14/2024 Zebra Devices on Android 13 Security Target Version 0.4, 07/26/2024 | Administrator Guidance for Zebra Devices (6375), Version 0.4, 06/14/2024 Zebra Devices on Android 13 Security Target Version 0.4, 07/26/2024 No changes, |
| Administrator Guidance for Zebra Devices (6490/5430), Version 0.4, 06/14/2024 | Administrator Guidance for Zebra Devices (6490/5430), Version 0.5, 02/14/2025<br>Updated the 6490/5430 document to identify the new product models. |

## Assurance Continuity Maintenance Report:

Zebra Devices submitted an Impact Analysis Report (IAR) to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on 13 March 2025. 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 2.0. 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 consists of the Security Target, the Supplemental Administrative Guidance, and the IAR. The ST and guide document were updated.

## Equivalent Models Added

Five equivalent models shown in the table have been added to the evaluated configuration:

| Model # | CPU | Micro-architecture | OS/Kernal | Wireless Chip Set |
|---|---|---|---|---|
| **TC27** | **Qualcomm QCM5430** | **ARMv8** | **Android 13.0/ Kernel 5.4** | **WCN6856** |
| **TC73-CR** | Qualcomm QCM5430 | ARMv8 | Android 13.0/ Kernel 5.4 | WCN6856 |

| | | | | |
|---|---|---|---|---|
| **TC78-CR** | Qualcomm QCM5430 | ARMv8 | Android 13.0/<br>Kernel 5.4 | WCN6856 |
| **EM45** | Qualcomm QCM5430 | ARMv8 | Android 13.0/<br>Kernel 5.4 | WCN6856 |
| **HC25** | Qualcomm QCM5430 | ARMv8 | Android 13.0/<br>Kernel 5.4 | WCN6856 |
| **HC55** | Qualcomm QCM5430 | ARMv8 | Android 13.0/<br>Kernel 5.4. | WCN6856 |

All the new models are equivalent to the evaluated model TC27. All new models have the same CPU, microarchitecture. OS, and wireless chip set as the TC27 evaluated model. All the hardware/Wi-Fi algorithm certificates have already been accepted and all cryptographic software remains unchanged, so all algorithm certificates remain valid, and no new certificates are required.

### Zebra Product Updates

There are a very large number of addons, updates, and bug fixes. These changes are non-security relevant. The changes do not impact the portions of the product implementing the SFR-related functionality. The updates are considered minor as they do not impact the security mechanisms of the TOE. The changes were less than 1 percent of the code of the product. The following table summarizes these changes by category.

| Category | Summary | Number of fixes |
|---|---|---|
| Platform | Interfacing with platform | 45 |
| OSX | Component in board support package (BSP) | 30 |
| WWAN | Wireless wide area network related | 133 |
| TUT | Tools and Utilities related | 26 |
| Datawedge | Data Capture mgt | 31 |
| Workstation Connect | Workstation extension (mouse, keyboard, etc.) | 43 |
| Core OS Connectivity | General networking | 21 |
| Fusion WLAN | WLAN mgt | 50 |
| Scanner | Scanner related | 51 |
| WorryFreeWifi | WiFi utility | 79 |
| Audio | acoustics related | 32 |
| OSUpdate | Updating the OS related | 2 |
| Bluetooth | Bluetooth related | 13 |
| RXLogger | logging utility | 42 |

| | | |
|---|---|---|
| MXProxy | Device mgt and configuration | 64 |
| FEAT | New Feature related | 99 |
| General | Removing dead code, battery performance and specific app bugs (e.g. data analytics app, zebra device manager app) | 238 |

### TOE Environment

There are no updates to operational environment components identified. The TOE environment is consistent with the validated results from the previous evaluation.

### Regression Testing

Zebra performs regression testing on each product version. This includes testing designed to address any CC related issues. Zebra implements a rigorous regression testing protocol for all modifications integrated into the product. This testing regimen encompasses both security assessments and functional evaluations. Zebra maintains a comprehensive test suite that is executed on a daily basis, with developers being accountable for validating their changes through testing prior to their incorporation into the main build.

### NIST CAVP Certificates:

The updates made to the TOE have not changed the cryptographic modules algorithm implementation nor their tested operational environment, so there is no impact to the CAVP certificates.

### Vulnerability Assessment:

The National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), and the Vulnerability Notes Database (http://www.kb.cert.org/vuls/) was searched on 3/13/2025 with the following search terms: "Android", "Android 13", "BoringSSL", "Android Locksettings service KBKDF", "QTI Crypto Engine Core", "QTI Inline Crypto Engine", "QTI Random Number Generato", "Zebra Technologies Corporation", "Zebra", "CC600", "CC6000", "ET40", "ET40HC", "ET45", "ET45HC", "ET51", "ET56", "ET60", "ET65", "HC20", "HC50", "L10A", "MC20", "MC9300", "PS20", "TC15", "TC21", "TC21-HC", "TC22", "TC26", "TC26-HC", "TC27", "TC52", "TC52-HC", "TC52ax", "TC52x", "TC52x-HC", "TC53", "TC57", "TC57x", "TC58", "TC72", "TC73", "TC77", "TC78", "TC83", "TN28", "VC83", "WT6300", "SD660", "SDM6375", "QCM5430", "QCM6490", "WCN3990", "WCN3980", "BCM43752", "WCN3988", "WCN6856", "TC73-CR", "TC78-CR", "EM45", "HC25", "HC55".

Note the terms TC73-CR, TC78-CR, EM45, HC25, HC55 were added to address all new devices.

There were no known vulnerabilities discovered in the product. Also, the IAR also had an embedded spreadsheet showing CVE issues from monthly Google Security Bulletins. These security bulletins are released monthly from Google and specify security patches for the CVEs. Vendors are expected to apply the patches to their Android devices.  Zebra has applied all of these patches.

## Conclusion:

CCEVS reviewed the description of the changes and the analysis of the impact upon security and found them all to be minor. No functionality, as defined in the SFRs, was impacted, and none of the product changes and vulnerability updates affected the security functionality or the SFRs identified in the Security Target. Therefore, CCEVS agrees that the original assurance is maintained for the product.