Release Notes – Zebra MC40 Android KK FIPS - BSP v02.13.0701 - LifeGuard Update 05 Release

Contents

Introduction

This release contains following software package which is compatible for MC40 KK FIPS Product.

LifeGuard patches are cumulative and include all previous fixes that are part of earlier patch releases

- **CFE-MC40N0-K-F0-070116-N-00-05.zip**

  Note: This LifeGuard CFE Package **CFE-MC40N0-K-F0-070116-N-00-05.zip** file is applicable only for FIPS SKU

This release package contains following fixes and patches.

- **Android Security Patch level:**
  - **February 2016 (Critical Patch level: Sept'17)**

    Use the link to refer the Android Security bulletin for more information: https://source.android.com/security/bulletin/

- **Fixes:**

  CFE v5:

  Corrections for KRACK vulnerabilities applied.

CFE v4:

- Updated the below Component's Version
  - MxMF version: 6.3.1.101
  - DataWedge: 6.4.18
  - EMDK Service: 6.5.12.812
  - StageNow: 2.7.2.1039

Resolved an issue in MX to prevent leakage of configuration parameters.

Included fix for Blueborne vulnerability.

SPR31550 – Mspclient.apk has been renamed to com.symbol.msp.apk

SPR32365 - Resolved an issue wherein the Scanner being enabled throughout reboot.

SPR32308 - Resolved an issue wherein scanner was unable to scan interleaved 205 type of barcodes.

CFE v3:

- Component's version
  - MxMF version: 5.0.1.4
  - DataWedge: 6.2.23
  - EMDK Service: 4.1.2.0
  - StageNow: 2.2.1.1455

SPR32008 - Resolved an issue wherein scanning PDF417 barcodes which contain embedded 0x0D characters resulted in continuous line of data instead of displaying in different lines.

SPR32126 - Resolved an issue wherein Stock Browser gets enabled automatically after reboot even though user has disabled the app in settings.

SPR32135 - Resolved an issue wherein Settings screen does not revert to its normal state even though the locale language is changed Arabic to English via EMDK.

SPR31650 - Resolved an issue wherein InputMethodService was causing junk character being read out in customer application

SPR32346 - Resolved an issue wherein proximity sensor's sensitivity was very high compared to other hardware

SPR32439/SPR32541 - Resolved an issue wherein the certificates get deleted Intermittently from the device, causing the device connectivity failures to N/W.

SPR31358/SPR31071 - Fixed an issue where the WLAN radio disconnects or falls back to "FT over Air" when "FT over DS" option is enabled in 802.11r.

SPR32193/SPR32230 - Resolved an issue wherein devices experiencing authentication failures, and were not able to recover.

CFE v2:

SPR31203 - Resolved an issue wherein the audio volume is degraded during VOIP calls

SPR30458 - Resolved an issue wherein Toggling Wi-Fi ON/OFF repeatedly causes a Kernel Panic and reboot.

SPR31243 - Resolved an issue wherein user is unable to answer incoming VOIP calls.

CFE v1:

SPR29349/SPR29390 - Resolved an issue wherein some of the audio packets were missing at the beginning of the call on REV B/REVB+ hardware.

SPR29076 - Resolved an issue wherein the network popup "the network might be monitored by 3rd party" displayed in the device during certificate installation

SPR29115 - Resolved an issue wherein the device resulting in to factory reset when it fails to unlock after some attempts.

SPR29787 - Added Proxy Wildcard support.

SPR29232 - Resolved an issue wherein the device display randomly goes off.

SPR29796 - Resolved an issue wherein ‘Android TransactionTooLargeException’ issue was seen

SPR29951 - Resolved an issue wherein VPN connection is unstable over WAN.

SPR29735 - Resolved an issue wherein the device reboots continuously after upgrading to KK from JB.

SPR30140 - Resolved an issue wherein the particular application installation fails, the only solution was to factory reset the device to install particular application

SPR30157 - Resolved an issue wherein the device reboots intermittently

SPR30259 - Resolved an issue wherein the device random reboot was observed over WLAN

SPR29912 - Resolved an issue wherein certificates installation failed through StageNow

SPR29945 - Fixed an issue wherein there was a delay in the output when scanning QR

code which have 100 characters onwards when using Keystroke output option.

SPR30417 - Resolved an issue wherein the device randomly stuck at splash screen

SPR30025 - Resolved an issue wherein the device experience the audio disruption during VOIP call

SPR30400 - Included configurability option to enable/disable network monitor warning pop-up messages.
> To Disable Warning you need to place a file namely ‘networkinfo.txt’ populated with content Value=false into /enterprise/usr/ path and reboot the device for the change to apply.
> To Enable Warning back (in case you had disabled it earlier) you need to place a file namely ‘networkinfo.txt’ populated with content Value=true into /enterprise/usr/ path and reboot the device for the change to apply.

SPR30402 - Resolved an issue wherein the device wherein does not notify the Access Point about power save while roaming.

SPR30401 - Added support to get the CFE version for MDM clients

SPR30472 - Resolved an issue wherein the device is not updated with latest date and time after critical suspend

SPR30435 - Resolved an issue wherein the device fails sometimes to roam to APs
MC-140261 - Resolved an issue wherein the devices with focal touch TP (REVB/REVB+) HW, if a user taps on the touch panel while the device is booting up, the device gets struck upon zebra splash screen

MC-143365 - Resolved an issue wherein binder crash observed due to dead object exception

SPR30916 - Resolved an issue where the device display would go blank on running customer camera application.

SPR31036 - Resolved an issue wherein MC40 was experiencing high degree of disruption to voice quality during VOIP calls.

Component Description and Version

Component / Description	Version
Product Build Number	02-13-12-4AJ22-K-F0-M1-070116
Android Version	4.4.4
WI-FI	**FUSION_A_4.01.0.0.017**

Package Details

CFE-MC40N0-K-F0-070116-N-00-05.zip

Note: This CFE package includes previous and new SPR fixes.

Device Compatibility

This LifeGuard CFE Package software release has been approved for use with the following Zebra devices.

Device P/N FIPS SKU	Operating System
MC40N0-HCJ3R01F	KitKat 4.4.4
MC40N0-HLK3R01F	
MC40N0-HLK3R02F	

Installation Requirements

This SW is intended for the MC40 KK device running on **02-13-12-4AJ22-K-F0-M1-070116** FIPS build only.

- ADB installed on the PC (including adb drivers)
- USB debugging turned ON (from Developer options)

Installation Instructions

1. Connect the USB cable from your PC to the device.
2. On your PC, you should see REMOVABLE DISK appearing in the File Explorer. copy the **CFE-MC40N0-K-F0-070116-N-00-05.zip** file on storage.
3. Put the MC40 into Recovery Mode using the following steps:
    - Hold the Power Key until “Reset” option appears, then release the power key.
    - Tap the “Reset” option in the menu and then immediately hold the "Power key" and "Scan Key” until the Zebra boot screen is displayed.
4. Once on the Recovery Screen, scroll up/down using “Volume Keys” +/- to "Apply update from internal storage" and press the “Scan Key” to select.

5. Next, scroll up/down using “Volume Keys” +/- to the location where you copied the files and press the “Scan Key” to select the desired folder.
6. Highlight the zip file you wish to install, and press the "Scan key" to select.

There are two ways to Check the Android Patch Level after install the CFE package in the device,

- ✓ Settings->About Device-> Zebra Patch Version: **CFE-MC40N0-K-F0-070116-N-00-05**
- ✓ Run “getprop persist.sys.cfe.patchver” command in ADB Shell.
  CFE-MC40N0-K-F0-070116-N-00-05

Release Date

Nov 2017