MC40 ANDROID KK - BSP V02.13.0701 - HOTFIX CFE V00.04 PACKAGE RELEASE NOTES

INTRODUCTION

HotFix CFE (Cumulative Fixes from Engineering) Package contains multiple SPR Hotfixes into a single package. The HotFix CFE Package helps the end users to keep up to date with all the SPR Hotfixes for given product software release / revision.

HotFix CFE packages are validated only by engineering validation team and the package follows Zebra Technologies HotFix Package Policy.
HotFix Support Policy

COMPONENT DESCRIPTION AND VERSION

Component / Description	Version
Product Build Number	02-13-12-4AJ22-K-V0-M1-070116
Android Version	4.4.4
Linux Kernel	3.4.48
Android SDK Level	19
Android security patch level	2016-02-01
Bluetooth Stack	4
Flash Size	8 GB
RAM Size	1 GB
MSP Agent/RD	7.08.85
Scanning Framework	6.23.0
Datawedge	3.3.15
DWDemo	2.0.7
Camera	6.23.0

OSX/MXMF	TI_OSX_4.5-2, 5.0.1.4
Wi-Fi	FUSION_A_4.01.0.0.011
PTT	3.1.20
RxLogger	3.0.0.52
MLogManager	MLogManager v06.52
Touch FW	0.14(RevB), 19 (RevC TPK),38(RevB+), 130 (RevB+ TPK_GFF)
EA	2.54
SPAM	0.6 (NA for RevC HW, only for RevA/B HW)
StageNow	2.2.1.1445
B2M Elemez	1.0.0.260
Data Analytics	1.0.2.1495
App Gallery	2.2.0.1
SOTI	12.2.0 Build 23434
EMDK	4.0.4.0
ZVC	1.1.15

FIXES/PATCHES INCLUDED:

Fixes Included:

The CFE Package **CFE-MC40N0-K-V0-070116_N_00_04.zip** file includes the following HotFixes:

SPR29349, SPR29390	-Fixed an issue wherein the audio packets were missing at the very beginning of the call on REV B/REVB+ hardware
SPR29076	-Provided a way to disable/enable "the network might be monitored by 3rd party"

alert that gets displayed upon installing user certificates.

SPR29115	-Fixed an issue wherein the devices used to incorrectly calculate no. of incorrect attempts to unlock the device resulting in factory reset of the device
SPR29787	-Fixed an issue wherein placing of wild card characters at the middle or end of the URL string was not allowed
SPR29232	-Fixed an issue wherein devices used to get randomly struck in black screen upon performing animations
SPR29796	-Fixed an issue wherein the framework incorrectly or vaguely reports the 'TransactionTooLargeException'
SPR29951	-Fixed an issue wherein intermittently the VPN connectivity was not stable
SPR29735	-Fixed an issue wherein few devices used to get into continuous reboots upon upgrading to KK from JB
SPR30140	-Fixed an issue wherein the application installation fails due to FAILED_UID_MISMATCH error requiring a data-wipe to overcome this issue
SPR30157	-Fixed an issue wherein device experienced reboot due to null pointer dereference
SPR30259	-Fixed an issue wherein device encounters random reboots while roaming in 802.1x infrastructure.
SPR29912	-Fixed an issue where certain certificates failed to install through Stage Now
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
SPR30147	-Fixed the issue wherein the device was randomly getting stuck to splash screen while going through a reboot
SPR30400	-Disabled the Network Monitor warning pop-up so that the warning doesn't come when the 3rd party certificate is installed (Configurability will be added and enabled by default)
SPR30402	-Fixed an issue wherein MC40 does not notify the Access Point about power save while roaming
SPR30401	-Created an application which reads the system properties and provide that to the MDM to allow it to get CFE version and other information
SPR30472	-Fixed an issue wherein the device would show incorrect date & time after a critical suspend
SPR30435	-Fixed an issue where fails to roam to APs
MC-140261	-Fixed an issue wherein the device would randomly get struck on splash screen on REVB+ hardware housed with Focal Tech Touch Panel
SPR30916	-Resolved issue wherein the device Display goes Black and Device is in not usable state on using customer camera app, Error handling in set_dss_ovl_info (Display

Subsystem)

SPR31036 - Resolved issue in MC40 is experiencing high degree of disruption to voice quality during VOIP calls.

Patches included:
- Security Patch CVE-2015-1805

This HotFix CFE package **CFE-MC40N0-K-V0-070116_N_00_04.zip** obsoletes the following HotFix CFEs:

HotFix CFE version	Product
CFE-MC40N0-K-V0-070116_N_00_02.zip	MC40
CFE-MC40N0-K-V0-070116_N_00_03.zip	

Note: Latest CFE package includes previous and new SPR HotFixes.

PACKAGE DETAILS:
CFE-MC40N0-K-V0-070116_N_00_04**.zip**
DEVICE COMPATIBILITY

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

Device	Operating System	BSP Version
MC40 KK Voice SKU	Android KK Version 4.4.4	v02.13.0701

INSTALLATION REQUIREMENTS

This SW is intended for the MC40 KK device running on 02-13-12-4AJ22-K-V0-M1-070116 Voice build only.

INSTALLATION INSTRUCTIONS

1. Connect the USB cable from your PC to the device.

2. Make sure MTP mode is selected in the device USB settings and MTP drivers are installed in your PC.

3. The internal SD card of MC40 will be seen in your PC as mounted drive MC40N0.

4. Copy the recovery update zip file "**CFE-MC40N0-K-V0-070116_N_00_0**4**.zip**" to the root folder on internal SD card.

5. Press and hold the Power button on the device until the Device options menu appears.

6. Tap on Reset to reboot the device.

7. When the device is rebooting hold the left Scan/Action button to enter Recovery update mode.

8. When the Recovery Mode home screen (Android logo) appears then release the left Scan/Action button.

9. Touch Home button to enter Recovery menu screen.

10. Click on Vol+ or Vol- to navigate to the "apply update from sdcard" option.

11. Click on PTT key to select the option.

12. Click on Vol+ or Vol- to navigate to the recovery update zip file.

13. Click on PTT key to select the recovery update zip file "**CFE-MC40N0-K-V0-070116_N_00_04.zip**".

14. Click on Vol+ or Vol- to navigate "reboot system now" and Click on PTT key to reboot the device.

15. There are two ways to Check the Android Patch Level after install the CFE package in the device,
- Settings->About Device-> Zebra Patch Version

- Run "getprop persist.sys.cfe.patchver" command in ADB Shell.

RELEASE DATE

Jan, 2017