MC40 OPERATING SYSTEM VOICE BSP 01.12.1012 REV. A RELEASE NOTES

INTRODUCTION

MC40N0 KK Voice SKU Patch Update v01.12.1012 includes critical security and vulnerability patches along with inclusion of Browser performance improvement fix.

This software is intended to be installed on the MC40N0 Voice SKU or NonVoice devices loaded with MC40 KK RevA OS v01.12.0720.

COMPONENT DESCRIPTION AND VERSION

Component / Description	Version
Product Build Number	01-12-06-4AJ22-K-V0-M1-101215
Android Version	4.4.4
Linux Kernel	3.4.48
Android SDK Level	19
Bluetooth Stack	4
Flash Size	8 GB
RAM Size	1 GB
MSP Agent/RD	7.08.85
Scanning Framework	5.25.0
Datawedge	3.1.20
DWDemo	2.0.6
Camera	5.25.0
OSX/MXMF	TI_OSX_4.4-3 , 4.4.3.6
Wi-Fi	FUSION_A_4.00.0.0.033

PTT	3.1.19
RxLogger	3.0.0.51
MLogManager	MLogManager v06.52
Touch FW	0.14(RevB), 19 (RevC TPK),38(RevB+)
EA	2.54
SPAM	0.6 (NA for RevC HW, only for RevA/B HW)
StageNow	2.1.1.1306
B2M Elemez	1.0.0.238
Data Analytics	1.0.1.2107
App Gallery	2.1.0.1
SOTI	12.2.0 Build 23434
EMDK	3.1.38
ZVC	1.1.5

FIXES/PATCHES INCLUDED:

Fixes included:

- Include changes for Browser Webkit to improve rendering performance

Patches included:

- CVE-2015-6609: Remote Code Execution Vulnerability in libutils.
- CVE-2015-6608: Remote Code Execution Vulnerabilities in Mediaserver.
- CVE-2015-1474: Integer overflow cause heap corruption in SurfaceFlinger
- CVE-2014-4943: Arbitrary kernel code execution via PPPOL2TP
- CVE-2015-3825: OpenSSLX509Certificate: mark mContext as transient.

- CVE-2015-6600: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-3867: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-3868: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-6603: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-6604: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-3876: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-6601: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-3871: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-3873: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-3823: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-6599: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-3869: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-6598: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-3870: Vulnerabilities in libstagefright Could Allow Remote Code Execution
- CVE-2015-3874: Vulnerabilities in Sonivox Could Allow Remote Code Execution

· CVE-2015-6602: Vulnerabilities in libutils Could Allow Remote Code Execution

· CVE-2015-3875: Vulnerabilities in libutils Could Allow Remote Code Execution

· CVE-2015-3877: Remote Code Execution Vulnerability in Skia

· CVE-2015-3872: Vulnerabilities in libstagefright Could Allow Remote Code Execution

· CVE-2014-3153: futex-prevent-requeue-pi-on-same-futex.patch

· CVE-2015-3863: Buffer overflow in Keystore handling of Blob objects

· CVE-2015-3858: Any 3rd party app can bypass the SMS short code notification prompt

· ANDROID-21141820: Check for special char when renaming device for Wi-Fi direct.

· CVE-2015-3861: Out of bounds read in MatroskaExtractor addVorbisCodecInfo() can crash the mediaserver process.

· CVE-2015-1534: Binder kernel driver DoS and potential kernel memory leak exploit

· CVE-2015-3849: Integer overflow in Region_createFromParcel in Region.cpp.

· ANDROID-17265206: Buffer overflow in libskia

· ANDROID-19507636: libpng buffer overwrite in png_build_index.

· ANDROID-17262540, ANDROID-17265466: Memory corruption can occur when calling libskia’s ICO

· CVE-2015-1528: Integer Overflow in libcutils.

· ANDROID-16794553: ArrayMap append() method can create duplicate entries in Bundle objects.

· ANDROID-15829193: Execute arbitrary code as any uid >= 1000 from adb shell

· CVE-2015-1536: Vulnerability in Bitmap unmarshalling.

· CVE-2015-0973: Vulnerability in libpng: Overflow in png_Read_IDAT_data.

· CVE-2015-1542: Universal XSS with View intent in Android Browser and WebView

· ANDROID-15428797: MediaFocusControl builds PendingIntent using its own uid and can send broadcast to any component.

· ANDROID-15288755: Sqlite race conditions leads to world-readable permissions.

· CVE-2015-3636: Use-after-free vulnerability in kernel handling of ping sockets.

· CVE-2015-1538, CVE-2015-1539: Integer overflow vulnerabilities in libstagefright.

CONTENTS

1. M40N0KXXXRE0000001.zip – Enterprise Reset Recovery Package

2. M40N0KXXXAE0000001.apf – Enterprise Reset AirBeam Package

3. M40N0KXXXRF0000001.zip - Factory Reset Recovery Package

4. M40N0KXXXAF0000001.apf - Factory Reset AirBeam Package

5. M40N0KXXXRW0000001.zip – Full Factory Reset Recovery Package

6. M40N0KXXXAW0000001.apf – Full Factory Reset AirBeam Package

7. M40N0KXXVRUxx20311.zip - MC40N0 KK RevB Voice SKU Recovery OS update package

8. M40N0KXXVAUxx20311.apf - MC40N0 KK RevB Voice SKU AirBEAM OS update package

9. M40N0KXXVRBxx20311.zip - MC40N0 KK RevB Voice SKU Recovery Upgrade package for JB to KK OS upgrade

10. M40N0KXXVABxx20311.apf - MC40N0 KK RevB Voice SKU AirBEAM Upgrade package for JB to KK OS upgrade

11. M40N0KXXVRPXX20311.zip - MC40N0 KitKat RevB Voice SKU Recovery OS diff update patch from RevA v01.12.0720 to RevB v02.13.0311

12. M40N0KXXVAPXX20311.apf - MC40N0 KitKat RevB Voice SKU AirBEAM OS diff update patch from RevA v01.12.0720 to RevB v02.13.0311

DEVICE COMPATIBILITY

This software release has been approved for use with the following devices.

Device P/N	Device P/N	Operating System
Voice SKU	**Non-Voice SKU**	KitKat 4.4.4
MC40N0-BCG3R01	MC40N0-BCG3R00	-
MC40N0-BCG3RM1	MC40N0-BCG3RM0	-
MC40N0-RCG3R01	MC40N0-RCG3R00	-
MC40N0-RCG3RM1	MC40N0-RCG3RM0	-
MC40N0-SCG3RM1	MC40N0-SCG3RM0	-
MC40N0-SCG3R01	MC40N0-SCG3R00	-
MC40N0-BCJ3R01	MC40N0-BCJ3R00	-
MC40N0-BCJ3RM1	MC40N0-BCJ3RM0	-
MC40N0-RCJ3R01	MC40N0-RCJ3R00	-
MC40N0-RCJ3RM1	MC40N0-RCJ3RM0	-
MC40N0-SCJ3RM1	MC40N0-SCJ3RM0	-
MC40N0-SCJ3R01	MC40N0-SCJ3R00	-
MC40N0-HCJ3R01	MC40N0-HCJ3R00	-
MC40N0-SLK3R01		-
MC40N0-SLK3RM1		-

MC40N0-HLK3R01		-

INSTALLATION REQUIREMENTS

1. The Software update requires Voice or Non-Voice SKU hardware device

INSTALLATION INSTRUCTIONS

Recovery Update procedure:

1. Connect the USB cable from your PC to the device
2. Make sure MTP mode is selected in the USB settings in the device 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 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 on PTT key to select the option
12. Click on Vol+ or Vol- to navigate to the recovery update zip file
13. Click on on PTT key to select the recovery update zip file
14. Click on Vol+ or Vol- to navigate “reboot system now” and Click on PTT key to reboot the device

- OS AirBEAM Update package

Please refer Mobility Service Platform deployment guide for instruction.

Note: Battery must be 30% charged to perform update

PART NUMBERS

1. M40N0KXXXRPXX11012.zip
2. M40N0KXXXAPXX11012.apf
3. M40N0KXXXRDXX11012.zip
4. M40N0KXXXADXX11012.apf

RELEASE DATE

Oct 20, 2015