TC55 OPERATING SYSTEM FOR GSM GMS DEVICES BSP 2.65FG FIPS DAR RELEASE NOTES

INTRODUCTION

TC55 is a ruggedized device based on Android for the enterprise market that blends the capabilities of a smart phone with those of a traditional enterprise PDA. TC55 has a number of enterprise-grade features, including a touch-screen that can be used with gloves, support for stylus input for signatures, barcode capture capability and IP67 rating for dust and water protection.

It also features Zebra Extensions (MX) to make the Android operating system more enterprise ready, with security enhancements and hooks for device management tools, and is designed for a longer lifecycle than the typical smart phone.
TC55 is designed in response to customer feedback from using consumer-grade smart phones in the workplace, especially with the bring-your-own-device (BYOD) trend, where employees use their own choice of device for work.

With TC55 the workers can capture practically any type of data — from bar codes and signatures to photos, videos and NFC — improving on the job efficiency and customer service. The screen is optimized for Enterprise viewing, helping ensure the battery lasts a full shift.
And with a drop, tumble and environmental sealing specification you can count on, it has the durability required to serve your field workers for years.

This SW release contains TC55 Android KitKat Rebranded SW version offering new advanced features, increasing operation performance for the customer satisfaction.

New Features in this Release

APA Features for TC55 KK:

1. Zebra Volume Control (ZVC) is an APA directive to standardize volume control for all Android products (KitKat and newer). ZVC replaces the default Android volume control which is accessible from Settings->Audio->Volume. When working in conjunction with AudioVolUIMgr CSP, ZVC also provides a means for our customers' IT administrator to put upper and lower limits on the volume sliders to prevent users from changing volume to the lowest or highest settings.

2. Extended Battery Information APA feature adds to and standardizes battery information presented to user in "Battery Information" UI. Information will include the critical parameters of the battery.

3. NONSD CARD STORAGE PATHS: Way to define and enforce a standard that ensures that the experiences of using these built-in areas, that are transient (e.g. /data) and persistent (e.g. /enterprise) and the folders within them are as similar as possible across devices for device users, application developers, and device administrators.

4. APA DHCP options: Gives the user a way to configure various DHCP options via CSP

5. APA OTA packaging: User will have the option to upgrade and downgrade between BSPs with incremental/rollback packages.

6. FIPS DAR Support.

Persistence feature: Whole enterprise folder is persisted across upgrade from JB to KK customers. Persistence of User configuration is supported via MDM only.
SPR Fixes:
28385 - Customer needs a solution to change the device hostname. Port of SPR#26191

28007 - JB to KK upgrade 02.52 Stagenow / MX not working an Factory Reset currently not detailed in RN is needed to get everything working

28182 - TC55/v2.52 StageNow Config will cause MX framework to fail, only resolvable with factory reset.

28374 - TC55 KK + EHS: NFC does not work after a reboot, screen lock/unlock sequence needed to restore NFC functionality

27835 - DataWedge GS1 Security Level - Invalid setting, and un-settable setting

28334 - TC55KK NFC Tags not reading in application, worked in JB Builds

28174 - TC55/GMS/2.52.02G.07 can’t access /enterprise/usr folder through any means

27587 - TC55 DNS not accessible over VPN - following of SPR#27543

28504 - EHS interfere with scan key setting

Security Patch Info:

CVEs	Comment

CVE-2015-3829	Integer overflow in libstagefright processing MPEG4 covr atoms when chunk_data_sizeis SIZE_MAX.
CVE-2015-3827	Integer underflow in libstagefright when processing MPEG4 covr atoms.
CVE-2015-3824	Integer overflow in libstagefright when parsing the MPEG4 tx3g atom.
CVE-2014-8610	Externally Reported Low Severity Security Vulnerability: SMS Resend Vulnerability in Android.
CVE-2014-8609	SECURITY: Don't pass a usable Pending Intent to 3rd parties.
CVE-2014-8507	Externally Reported Moderate Security Issue: SQL Injection in WAPPushManager.
CVE-2014-7911	Add additional checks in ObjectInputStream.
CVE-2015-3873	Vulnerabilities in libstagefright Could Allow Remote Code Execution
CVE-2015-3872	
CVE-2015-3871	
CVE-2015-3868	
CVE-2015-3867	
CVE-2015-3869	
CVE-2015-3870	
CVE-2015-	

3823	
CVE-2015-6598	
CVE-2015-6599	
CVE-2015-6600	
CVE-2015-6603	
CVE-2015-6601	
CVE-2015-3876	
CVE-2015-6604	
CVE-2015-3874	Vulnerabilities in Sonivox Could Allow Remote Code Execution
CVE-2015-3875	Vulnerabilities in libutils Could Allow Remote Code Execution
CVE-2015-6602	
CVE-2015-3877	Remote Code Execution Vulnerability in Skia
CVE-2015-6608	The patch includes additional checks to validate word length.
	The patch includes additional checks to properly fail memory allocations and verify the size value used to allocate the memory that is read from a file.
CVE-2015-	Remote Code Execution Vulnerability in libutils

6609	
CVE-2015-1538	Integer overflows during MP4 atom processing
CVE-2015-1539	An integer underflow in ESDS processing
	SPR28147- StageFright Security Patch/ Android OS Vulnerable to Text Hack
CVE-2015-0973	Vulnerability in libpng: Overflow in png_Read_IDAT_data
	SIGSEGV in jmem-ashmem could cause remote code execution
CVE-2015-1536	Vulnerability in Bitmap unmarshalling
CVE-2015-3824	Integer overflow in libstagefright when parsing the MPEG4 tx3g atom
CVE-2015-3826	Unbounded buffer read in libstagefright while parsing 3GPP metadata allows reading arbitrary memory
CVE-2015-3827	Integer underflow in libstagefright when processing MPEG4 covr atoms
CVE-2014-6041	Multiple integer overflows in libstagefright SampleTable
CVE-2014-6041	MediaFocusControl builds PendingIntent using its own uid and can send broadcast to any component.
CVE-2014-6041	Execute arbitrary code as any uid >= 1000 from adb shell
CVE-2014-6041	ArrayMap append() method can create duplicate entries in Bundle objects
CVE-2014-6041	Memory corruption in libskia
CVE-2014-	Buffer overflow in libskia

6041	
CVE-2014-6041	Settings app allows sending protected broadcasts
CVE-2014-6041	sqlite race conditions leads to world-readable permissions
CVE-2014-0972	Unprivileged GPU command streams can change the IOMMU page table
CVE-2013-6282	Missing access checks in put_user/get_user kernel API
CVE-2015-3636	**SPR28252 - Use-after-free vulnerability in kernel handling of ping sockets**

Add GMS (Google Mobile Service) package. GMS package includes:

New Applications

· Chrome – Google's WWW browser

· Google – Search and Google Now

· Gmail – email client for gmail

· Google Docs / Drive – Access to Google Drive files

· Google Settings – Control Panel for Google apps, also Android Device Manager Access

· Google + - Google Social Networking

· Hangouts - Extension of Google+ for calls and videos and pictures

· Maps – Google Maps and Navigation

· Play Games – Buy games and play

· Play Newsstand – Buy multimedia magazines and newspapers

· Play Books – Buy, Store, and Read Books

· Play Music – Store, Play, Buy Music

· Play Movies and TV – Buy, Play, and Store Movies/TV Shows

· Play Store – Store and purchase Android Applications

· Voice Search – Voice driven web search

· YouTube – Video Sharing

Note: When connected to network, Google will determine local rules for GMS application in different countries (such as Play Books, Play Magazines, and Play Movies).

Updated Applications

· Calendar – Same as the AOSP Calendar application except it includes synchronizing Google Calendar Events.

· People - Same as the AOSP People application except it includes synchronizing Google Contacts.

DESCRIPTION

1. Android KitKat 4.4.3
2. Kernel 3.4.0
3. DataWedge v 3.1.29
4. Scanning Framework v5.46.0
5. MX.v4.4.4
6. WLAN FUSION_QA_1.02.0.0.028
7. RIL 1.0.10
8. Modem 20015326.48
9. MSP v07.08.85
10. SOTI client v12.1.0 Build 23469
11. StageNow v 2.1.1.1425
12. SimulScan v1.11.1
13. EMDK 3.1.38

CONTENTS

1. T55N0KF0VRUEN265G.zip – TC55 KK FIPS GMS OS Recovery Update package

2. T55N0KF0VREEN265G.zip – TC55 KK FIPS GMS Enterprise Recovery reset package

3. T55N0KF0VRFEN265G.zip – TC55 KK FIPS GMS Factory Recovery reset package

4. T55N0KF0VAUEN265G.apf – TC55 KK FIPS GMS OS Airbeam package for MSP deployment

5. T55N0KF0VAEEN265G.apf – TC55 KK FIPS GMS Airbeam package for Enterprise reset

6. T55N0KF0VAFEN265G.apf – TC55 KK FIPS GMS Airbeam package for Factory reset

DEVICE COMPATIBILITY

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

SKUs supported:

TC55AH-HJ11EE

INSTALLATION REQUIREMENTS

This SW is intended for the FIPS TC55AH devices

INSTALLATION INSTRUCTIONS

For upgrading from older version of KK

1. T55N0KF0VRUEN265G.zip – TC55 KK GMS OS Recovery Update package
    - Connect the USB cable from your PC to the device and enable USB mass storage mode on the device.
    - On your PC you should see an internal and SD card (if SD card is present) appears in the File Explorer and copy the recovery update zip file to any storage.
    - Press and hold on the device the Power button, Scan/Action button and Vol+ until the screen is turned OFF
    - Release the Power and Scan/Action buttons and continue to hold Vol+ button
    - The device should enter to Recovery update mode
    - Release Vol+.
    - Click on Vol+ or Vol- to navigate and select appropriated storage
    - Click on on Scan/Action button to select the option
    - Click on Vol+ or Vol- to navigate to the recovery update zip file
    - Click on on Scan/Action button to select the recovery update zip file
    - Reboot the device
2. T55N0KF0VRFEN265G.zip – TC55 KK GMS Factory Reset recovery package – Use only if you want to wipe Data and Enterprise partition
3. WLAN Region file Recovery update per Country Region – see the table below (not required for TC55 KitKat GMS devices out of factory)

Country Group (Region)	Country Codes	WLAN Region File

USA,	US,	TC55KKFCCWLNV07.zip
Canada,	CA,	
Puerto Rico,	PR,	
American Virgin Island,	VI,	
Anguilla,	AI,	
Cayman Islands,	KY,	
Guam,	GU,	
Mariana Islands,	MP,	
Dutch Antilles,	AN,	
Curacao,	CW,	
Bonaire, Saint Eustatius and Saba,	BQ,	
St Maarten,	SX,	
Taiwan,	TW,	

MSP OS package update

Please refer Mobility Service Platform deployment guide for instruction for the deployment of the following files:

1. 1. TC55 KK GMS OS Airbeam package
2. 2. TC55 KK GMS Airbeam package for Enterprise reset
3. 3. TC55 KK GMS Airbeam package for Factory reset

NOTES

a. Visual Voice Mail (VVM) is not supported for all carriers.

b. Enterprise Enabler is not needed for TC55 KK OS.

c. Once upgraded to KK, downgrade to JB is not supported.

PART NUMBER RELEASE DATE

1. T55N0KF0VRUEN265G.zip
2. T55N0KF0VRFEN265G.zip
3. T55N0KF0VREEN265G.zip
4. T55N0KF0VAUEN265G.apf
5. T55N0KF0VAFEN265G.apf
6. T55N0KF0VAEEN265G.apf

April, 2016