



Release notes for TC70 Android L LifeGuard Update 23 (GMS FIPS)

Aug 2022

Description

This release contains the following software package which is compatible with the TC70 GMS FIPS product. LifeGuard patches are cumulative and include all previous fixes that are part of earlier patch releases.

Component Contents

Package Name	Package Description
CFE-TC70-L-F0-021002-G-00-23.zip	CFE package update 23 for TC70 GMS FIPS

Component Version Info

Component / Description	Version
Product Build Number	02-10-02-LG-00-A release-keys
Android Version	5.1.1
Linux Kernel	3.4.0
Android SDK Level	22
Android security patch level	2018-03-05 (Critical Patch Level: 2022-08-01)
Platform	QC 8960 Pro
Bluetooth Stack	01.024.00
Flash Size	8GB
RAM Size	1GB

MSP Package	7.08.85
Scanner Framework	19.65.37.4
SimulScan Demo App	2.6
SimulScanEngine	1.13.6.5
Datawedge	6.7.51
EMDK	6.8.24.1124
OSX/ Mx	OSX QC.51.5.2.14/ MXMF version:7.2.10.3
Wi-Fi	FUSION_QA_2.00.0.0.029
PTT	3.1.27
Touch FW	STYLUS-80_GLOVE-105, FW:1.2. AA
RxLog	4.58.5.0
Mlog	v06.54 / Service v06.54
Bluetooth Pairing Utility	3.7
File Browser	Ver 1.19.12
Stage Now	2.10.1.1389
App Gallery	2.8.4.13
Tech Docs	1.0.0
WLAN	WLAN-1240294.1

NFC	NFC_NCIHAL_AR3.5.0_Lollipop, FW:122
Sensors (Accel, Gyro, Light, Prox)	1, 1, 1, 1
Camera	CAM-FRONT-1.0.0
MSRN	0.94
MobiControl	12.2.0. Build 23469
Zebra Volume Control	1.1.23
IST	App:1.00 build 3/Service: 1.00 build 1/Firmware:1.00 build 5
Battery Manger	1.3.6
DDT	1.15.0.11
FingerPrint	Zebra/TC70/TC70:5.1.1/02-10-02-LG-00-A/180316:user/release-keys
ZSL	3.1.1
Zebra Data Service	3.7.1.1003
EKB	1.7.0.5
WifiConfigCSP	7.0.1
License Manager	3.2.0

1. CFE v23 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-23.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: August 01, 2022)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

2. CFE v22 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-22.zip (GMS FIPS)

❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: February 01, 2022)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

3. CFE v21 Updates:

❖ CFE-TC70-L-F0-021002-G-00-21.zip (GMS FIPS)

❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: November 01, 2021)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- SPR45273 - CVE 2021-1048 Patched the use-after-free security vulnerability which could allow code execution and local elevation of privilege to the kernel from an untrusted application.

4. CFE v20 Updates:

❖ CFE-TC70-L-F0-021002-G-00-20.zip (GMS FIPS)

❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: Aug 01, 2021)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- SPR41487 - Resolved an issue wherein bugreport sometimes produces an error when uploaded to BatteryHistorian.
- SPR41907 - Resolved an issue wherein device use to stuck on boot screen in multi boot use case.
- Scanner Framework updated to 19.65.37.4
 - a. SPR44327/SPR43562 - Resolved an issue wherein scanner doesn't work after reboot when device enrolled in SOTI mode.
 - b. SPR41676 - Resolved an issue wherein devices are unable to scan dot matrix barcodes.

5. CFE v19 Updates:

❖ CFE-TC70-L-F0-021002-G-00-19.zip (GMS FIPS)

❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: May 01, 2021)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- SPR42956 – Resolved an issue wherein device cannot handle AP scan results when coming back from out of WiFi range.

6. CFE v18 Updates:

❖ CFE-TC70-L-F0-021002-G-00-18.zip (GMS FIPS)

- ❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: February 01, 2021)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

7. CFE v17 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-17.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: October 01, 2020)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- SPR39290 – Resolved an issue where TC70 faces Intermittent Loss of connection with Bluetooth headset.
- SPR38341 – Resolved an issue wherein device was getting stuck in boot loop as audio service was getting started a little late.

8. CFE v16 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-16.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: June 01, 2020)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- Added support for Tianma display panel.

9. CFE v14 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-14.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: Apr 01, 2020)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- SPR38404 - "Fixed an issue where there was screeching noise heard after a voip call, and RXDevice was switched to speaker"
- SPR38341 - Resolved an issue wherein device was getting stuck in boot loop as audio service was getting started a little late
- SPR37771 - Fixed an issue wherein the device was associated to an Access Point and does not roam.
- SPR33312 – Resolved an issue wherein certain StageNow profile was not able to use after upgrading from KitKat to Lollipop OS.
- SPR37434 – Resolved an issue wherein device heats up when the configuration is pushed as xml file from AirWatch or StageNow.
- SPR34353 - Resolved an issue of unexpected EOF exception in logcat.
- SPR 35766 - Resolved an issue wherein device takes longer time to connect when deployed in a denser SSID environment.

- SPR37272 - Resolved an issue wherein EHS Hostname in title was not reflecting updated Hostname after device reboot.
- SPR 34909 - Resolved an issue when device initiates a connection with Mesh BSSID
- SPR 32157 - Resolved an issue when an invalid Neighbor AP response received from the infrastructure.
- SPR39273 – Resolved an issue wherein device use to struck on zebra logo due to slimbus timeout on multiple warmboot.
- Updated following Components:
 - License Manager: 3.2
 - Zebra Data Service: 3.7.0.1004
 - WIFI: FUSION_QA_2.00.0.0.026

Known Issue:

On first boot-up after installing the LG CFEv14 patch, the Android OS installs the new ZDS (v3.x), which is conflicting with the old ZDS (v2.x) process which might have already started on boot complete. This is intermittent and one-time issue and does not have any impact on ZDS functionality or the OS

10. CFE v13 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-13.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: July 01, 2019)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- SPR36654 - Resolved an issue where TC70 experiences BT audio disconnect when WLAN 11d set to Auto.
- SPR36991 - Resolved an issue wherein with SKT SIM card device will connect to network but shows as No service.
- SPR37104 - Resolved a Framework reboot issue when user tries to access missed call message notification on user screen in EHS (MMS is disabled).
- SPR36971 - Resolved an issue wherein the device was sometimes sticking to Wi-Fi Access Points even at very low signal levels.
- SPR36633 - Resolve a scan failure issue when application using EMDK Timed Release api to scan the barcodes.
- SPR37258 - Resolved an issue where DNS Resolution fails when device roams to different subnet.
- Updated below mentioned components:
 - Scanner Framework: 19.56.37.2
 - WLAN: FUSION_QA_2.00.0.0.021

11. CFE v12 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-12.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: April 05, 2019)



Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- SPR35912 - Resolved an issue wherein 11k operation depends on 11r functionality
- SPR36265 - Fix an issue where scanning is not working after reconnecting the out of range RS507 by Bluetooth
- SPR35288 - Fixed an issue wherein initialization of scanner was taking ~1sec.
- SPR35054 - Added support for reduced quiet zone barcode decoding.
- SPR34844 - Resolved an issue wherein multiple open calls are prevented when multiple application tries to open scanner without releasing previous instance.
- Updated below mentioned components:
 - Scanner Framework: 19.53.37.0
 - Bluetooth: 01.018.00

12. CFE v11 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-11.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: December 05, 2018)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- SPR36118 – Resolved an issue wherein patch version was not updating in cfe.ini.
- SPR34738 – Resolved an issue wherein device reboots when VPN connection established over Cellular (AT & T).
- SPR35368 – Resolved an issue wherein scanner crash while scan the barcode just before suspend or after resume the device.
- SPR35362 – Resolved an issue to set hardware picklist to scan barcodes which are very close to each other.
- SPR33709 – Implemented the intercharacter delay functionality in Datawedge to support RDP session scan data transfer.
- SPR34191 – Resolved an issue where Devices not sending the hostname to the DHCP server.
- Updated below mentioned components:
 - MX: 7.2.10.2 (For detail please refer <http://techdocs.zebra.com>)
 - Scanner Framework: 19.12.35.0
 - EKB:1.7.0.5
 - Bluetooth: 01.015.00

13. CFE v10 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-10.zip (GMS FIPS)

❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: September 05, 2018)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- SPR35025 – Resolved an issue where Proxy Auto Config (PAC) did not work properly following stops/restarts of the PacService.
- SPR33977 – Resolved an issue wherein set time zone issue observed with StageNow.
- SPR34716 – Resolved an issue wherein the MX Framework did not restart properly following events where the service was stopped.
- SPR34679 – Resolved an issue wherein setting WiFi Band selection to Auto was not working properly with StageNow.
- SPR34936 – Resolved an issue wherein Datawedge used to crash on bootup.
- SPR31195 – Resolved an issue wherein pressing trigger key while in chrome browser with multiple tabs used to result in switching to a different tab.
- SettingsEULA has been renamed to Zebra Data Services.
- Updated below mentioned components:
 - MX: 7.2.9.0 (For detail please refer <http://techdocs.zebra.com>)
 - Scanner Framework: 19.10.35.1
 - ZSL:3.1.1
 - WifiConfigCSP:7.0.1

14. CFE v9 Updates:

❖ CFE-TC70-L-F0-021002-G-00-09.zip (GMS FIPS)

❖ **Android Security Patch Level:** March 05, 2018 (Critical Patch Level: June 05, 2018)

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- SPR33755 – Resolved an issue wherein the Whitelisted apps were unable to submit XML to MX.
- SPR33207 – Resolved an issue wherein the Device Diagnostic tool had an issue with reading the Battery Cycles in the application for PP+ batteries.
- SPR34267 – Resolved an issue where-in user was not able to enable USB debugging option using StageNow.
- SPR33862 – Fixed an issue where-in user could not set Display Timeout value of 30min using StageNow.
- SPR34145 – Fixed an issue wherein user was unable to connect to WLAN network due to WEP Key Index issue.
- SPR34307 – Resolved an issue wherein device out of the box intermittently failed to get staged via StageNow.

- SPR34083/34014/32519 – Resolved an issue wherein disabling WWAN radio via Airwatch using StageNow XML fails.
- SPR33639 – Resolved an issue wherein the customer app install and launch during device sleep state and device stop emitting scan beam after awake from suspend.
- SPR33876 – Resolved an issue wherein Display Timeout was unable set via StageNow.
- SPR33607 – Resolved an issue where few fresh devices were unable to stage after unbox the device.
- SPR33538 – Resolved an issue wherein the Scanner beam stuck off and No LED beam while pressing scanner button.
- SPR33981 – Resolved an issue Czech Republic Regulatory Country could not be set using Wifi config profile.
- SPR34429 – Resolved an issue wherein device failed to emit scan beam if the application was launched during device suspend.
- SPR34614 – Fixed an issue in DataWedge wherein scanner could not be enabled due to quick enabling and disabling of scanner through Intents.
- SPR34716 – Resolved an issue wherein the MX was getting killed by Backupmanager and didn't restart properly.
- SPR34213 – Resolved an issue wherein shared preference initialization without launching EKB.
- Added support for Enterprise Lockdown feature.
- Updated below mentioned components:
 - Datawedge: 6.7.48
 - EKB: 1.7.0.2 (Added as a System application with this CFE 09)
 - MX: 7.2.8.2

15. CFE v8 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-08.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** March 05, 2018

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- Spectre & Meltdown correction for variant 1 and variant 2
- SPR33599 - Resolved an issue wherein few of the system applications are getting disabled after enabling whitelist.
- SPR33799 - Resolved an issue wherein scanner was unable to read '\n' and '\r'.
- SPR33930 - Resolved an issue wherein dhcp address was not acquired by the device, while hostname is greater than 32 characters.
- SPR33823 - Resolved an issue wherein black screen occurred in DataWedge application.

- SPR33973- Resolved an issue wherein erroneously loading default profile by providing feature to ignore disabled profiles in DataWedge.
- SPR33671- Resolved an issue wherein user was unable to create WIFI profile with username as backslash followed by number.
- Updated below mentioned components:
 - Datawedge: 6.7.47
 - StageNow: 2.10.1.1389
 - EMDK: 6.8.21.1121
 - MX: 7.2.1.0
 - File Browser: 1.19.12
 - Diagnostic Tool: 1.15.0.11
 - Scanner Framework: 19.9.35.0
 - Radio: 2.00.0.0.009
 - Bluetooth: 01.12.00

16. CFE v7 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00--07.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** January 05, 2018

Use the below link to see the Android Security bulletin for more information:
<https://source.android.com/security/bulletin/>

17. CFE v6 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-06.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** December 05, 2017

Use the below link to see the Android Security bulletin for more information:
<https://source.android.com/security/bulletin/>

- SPR32825 - Resolved an issue wherein BT headset volume up/down was not working during Bluetooth call scenario.
- SPR33233 - Resolved an issue wherein the DataWedge 6.2.24 could not replace separator or non-printable ascii character with \$.
- SPR32463 - Resolved an issue wherein the StageNow File Manager downloads frequently fails due to Socketimeout exception.
- Updated below mentioned components:
 - Datawedge: 6.6.49
 - StageNow: 2.9.1.1344
 - EMDK: 6.7.10.1010

- MX: 7.1.1.0

18. CFE v5 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-05.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** September 05, 2017

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- Corrections for KRACK vulnerabilities applied.
- SPR30400/31340 – Added support to enable/disable Network Monitoring Notification.

19. CFE v4 Updates:

- ❖ CFE-TC70-L-F0-021002-G-00-04.zip (GMS FIPS)
- ❖ **Android Security Patch Level:** September 05, 2017

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- Updated below mentioned components:
 - MXMF - Version 7.0.2.1
 - DataWedge - Version 6.5.61
 - EMDK - Version 6.6.14.914
 - Staging Client - Version 2.8.1.1221
- Resolved an issue in MX to prevent leakage of configuration parameters.
- Included fix for BlueBorne vulnerability.
- Included fix for blank screen seen during boot.
- SPR32385 – Resolved an issue wherein Simulscan API fails to read Chinese passports.
- SPR32582 – Added support for Netherlands - Belgium language.
- SPR32008_SPR31820 – Resolved an issue wherein scanning PDF417 barcodes which contain embedded 0x0D characters resulted in continuous line of data instead of displaying in different lines.
- SPR32666 - Resolved an issue wherein device reboots when it roams from secured to open Wi-Fi network.
- SPR32676 – Resolved an issue wherein DataWedge App crashes when Velocity App tries to send an Intent to enable the scanner plugin.
- SPR32775 – Resolved an issue wherein the notification class created with FLAG_INSISTENT was not getting cleared upon pulling down the notification drawer.

20. CFE v3 Updates:

❖ CFE-TC70-L-F0-021002-G-00-03.zip (GMS FIPS)

❖ **Android Security Patch Level:** August 05, 2017

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- SPR29912 - Resolved an issue wherein certificates installation failed through stagenow.
- SPR30401 - Added support to get the CFE version via MDM clients.
- SPR31954 - Resolved an issue wherein dhcpd was not able to start due to lengthy host name.
- SPR31686 - Resolved an issue wherein dhcpd was not able to start due to lengthy host name.
- SPR32135 - Resolved an issue wherein Settings screen does not revert to its normal state even though the locale language is changed from Arabic to English via EMDK.
- SPR32240 - Resolved an issue wherein the scanner service was not responding while switching between applications.
- SPR32193/SPR32230 - Resolved an issue wherein devices experiencing authentication failures, and were not able to recover.
- SPR32539 - Resolved an issue wherein build certificates were lost randomly even though certificates were not expired.
- SPR32326 - Resolved an issue wherein Settings application crashed while trying to set enterprise keyboard as the default keyboard and disable AOSP keyboard through the stageNow profile.
- SPR32413 - Resolved an issue wherein after selecting the static option in the ethernet settings, changes are not reflecting in interface and the interface was always dhcp.

21. CFE v2 Updates:

❖ CFE-TC70-L-F0-021002-G-00-02.zip (GMS FIPS)

❖ **Android Security Patch Level:** July 05, 2017

Use the below link to see the Android Security bulletin for more information:

<https://source.android.com/security/bulletin/>

- Added Zebra patch version value in Settings to identify the CFE Patch version.

Note

Tianma display devices are not allowed to downgrade to any of the older BSPs or Patches

- To identify the display type on TC70 devices user can check the 'persist.sys.hw.display.id' property using adb getprop command.
 - For TC70 Innolux device [persist.sys.hw.display.id]: [600]
 - For TC70 Tianma device [persist.sys.hw.display.id]: [512]

CFE v15 was a beta release. However, devices can be updated from v14 to v16 or v15 to v16.

Full package update (FPU-TC70-L-F0-021002-G-00-16.zip) is mainly meant for TC70 Tianma display devices as these devices are not allowed to downgrade to any of the older BSPs.

Important Links

- **Requirements and Instructions**
 - [Installation and setup instructions](#)
- [Zebra Techdocs](#)
- [Developer Tools](#)

Device Compatibility

This software release has been approved for Android TC70 L GMS FIPS models mentioned below.

Device	Operating System
TC700H-GC11ES-NA	Android 5.1.1
TC700H-GC11ES-IN	Android 5.1.1
TC700H-GC11ES-IA	Android 5.1.1

Last Revised: 8th August 2022