Product name	Confidentiality level
B612s	CONFIDENTIAL
Product version	Total 9 pages
V1.0	

B612s-25dTCPU-V100R001B195D01SP00C842

Firmware Release Notes

V1.0

Prepared by	B612s team	Date	2018-03-06

Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2018.03.06	1	11.195.01.00.842	The 1st Version	B612s team

Table of Contents

1 Main Features 4
2 Hardware 4
2.1 Version Description 4
2.2 Hardware Specifications 4
2.3 Improvements in the Previous Version 6
2.4 Known Limitations and Issues 6
3 Firmware 6
3.1 Version Description 6
3.2 Firmware Specifications 6
3.3 Improvement in the Previous Version 7
3.4 Known Limitations and Issues 7
4 WebUI/HiLink 8
4.1 Version Description 8
4.2 WebUI/HiLink Specifications 8
4.3 Improvement in the Previous Version 8
4.4 Known Limitations and Issues 8
5 Software Vulnerabilities Fixes 8

Abbreviations	description

1 Main Features

The B612s mainly supports the following features:

- LTE Cat6 4*4 MIMO，FDD 300/50Mbps@20MHz，TDD 220/10Mbps@20MHz
- Data and SMS Service
- Support WiFi 2*2 2.4G; WIFI 802.11 /b/g/n,40MHz(11n)
- 4GE 1POTS
- WEB UI, Auto connect
- LED indicators

Windows XP SP3, Windows Vista SP1/SP2, Windows 7, Windows 8, Windows 8.1 (does not support Windows RT), MAC OS X 10.7, 10.8 and 10.9 with latest upgrades

2 Hardware

2.1 Version Description

Hardware Version: **WL1B612M01**

Platform & Chipset: Balong Hi6950

2.2 Hardware Specifications

Item		Specifications	
Technical standard		WAN: LTE	
		WLAN: IEEE 802.11b/g/n/ac	
Operating frequency	B612s-51d	LTE: Band2, Band4, Band5,Band7, Band28, Band38,Band41, Band42, Band43	
		UMTS: Band2,Band4 Band5	
		GSM : Band2, Band3, Band5, Band8	
		WiFi: 2.4G	
	B612s-25d	LTE: Band1, Band3, Band7,Band8, Band20,Band38,Band40, Band41, Band42, Band43	
		WiFi: 2.4G	
Maximum transmitter power		UMTS: NA	
		WLAN	802.11b: 16 (+/-3) dBm
			802.11g: 17 (+/-3) dBm

Item	Specifications	
		802.11n: 17 (+/-3) dBm
Receiver sensitivity	UMTS: NA	
	WLAN 802.11b	-83 dBm@11 Mbit/s
		-89 dBm@1 Mbit/s
	WLAN 802.11g: -69 dBm@54 Mbit/s	
	WLAN 802.11n: -67 dBm@65 Mbit/s	
WLAN speed	802.11b: Up to 11 Mbit/s	
	802.11g: Up to 54 Mbit/s	
	802.11n: HT40 MCS15(300Mbit/s), HT20 MCS15(144.4Mbit/s)	
Maximum power consumption	12 W	
Power supply	AC: 100–240 V	
	DC: 12 V, 1 A	
External interfaces	WAN/LAN: 4 RJ45,GE	
	SIM card interface: standard 6-pin SIM card interface	
Indicators	MODE:	cyan: 4G mode green: Ethernet WAN mode Red: No SIM/USIM card is found, the PIN is not verified, or the SIM/USIM card is not working properly. Failed to connect to a mobile network
	Signal	One to three: Weak to Strong signal Off: out signal
	WPS/WIFI	White Blink: WPS open On: WiFi is opened Off: WiFi is closed
	LAN	White Blink: Data transfer Off: No connect ether cable On: connect ether cable
	Power	On/Off
Button	Reset switch, WPS switch, Power switch	
Dimensions (D × W × H)	240mm*155mm*78mm	
Weight	about 600g (Does not contain the power adapter)	

Item	Specifications
Temperature	Operating: 0℃ to +40℃
	Storage: -20℃ to +70℃
Humidity	5% to 95% (non-condensing)

2.3 Improvements in the Previous Version

Index	Case ID	Issue Description
NA		

2.4 Known Limitations and Issues

Index	Case ID	Issue Description
NA		

3 Firmware

3.1 Version Description

Firmware Version:	11.195.01.00.842
Baseline information	BalongV700R500C31B195
OS	RTos / linux 3.10

3.2 Firmware Specifications

Item	Description
Network connection setup	• APN management: create, delete and edit. • Set up network connection
WLAN setup	• SSID broadcasting and hiding • Open system and shared key authentication • ASCII and HEX keys • 64/128-bit WEP encryption • 256-bit WPA-PSK and WPA2-PSK encryption • AES encryption algorithm • TKIP and AES integrated encryption algorithm • Automatic adjustment of ratios • Display STA status • WLAN MAC filter

Item	Description
Firewall setup	• Firewall Switch • LAN IP Filter • Virtual Server • DMZ Service
NAT setup	• CONE NAT • Symmetric NAT • ALG • VPN pass-through
DHCP setup	• DHCP server enabling and disabling • Address pool of the DHCP server setup • DHCP lease time setup
Other	• Automatic network selection and registration • Manual network selection and registration
	Network status display: signal, operator name, system mode, and so on.

3.3 Improvement in the Previous Version

Index	Case ID	Issue Description
1	WEBSDK-E-023-20-CUS	RSRQ:[enable] RSRP:[enable] SINR:[enable] CELL_ID:[enable]
2	REQ.008	Under "Aktuálne pripojenie:" please update the words to the following: Odoslané / Prijaté: Under "Stav WLAN" please update the words change to Zapnuté or Vypnuté

3.4 Known Limitations and Issues

Index	Case ID	Issue Description

4 WebUI/HiLink

4.1 Version Description

WebUI/HiLink Version:

4.2 WebUI/HiLink Specifications

Item	Specifications

4.3 Improvement in the Previous Version

Index	Case ID	Issue Description

4.4 Known Limitations and Issues

Index	Case ID	Issue Description

5 Software Vulnerabilities Fixes

[Software Vulnerabilities include Android Vulnerability, Third-party software Vulnerability, and Huawei Vulnerability]
[Android Vulnerability is from Google, which reported publicly.]

[Third-party software is a type of computer software that is sold together with or provided for free in Huawei products or solutions with the ownership of intellectual property rights (IPR) held by the original contributors. Third-party software can be but is not limited to: Purchased software, Software that is built in or attached to purchased hardware, Software in products of the original equipment manufacturer (OEM) or original design manufacturer (ODM), Software that is developed with technical contribution from partners (ownership of IPR all or partially held by the partners), Software that is legally obtained free of charge.
The data of third-party software vulnerabilities fixes can be exported from PDM.
If the table is excessively long, you can divide it into multiple ones by product version, or deliver it in an excel file with patch release notes and provide reference information in this section.]

[Huawei Vulnerability is Huawei own software' Vulnerability, which found by outside]

Vulnerabilities information is available through CVE IDs in NVD (National Vulnerability Database) website:

http://web.nvd.nist.gov/view/vuln/search

Software/Module name	Version	CVE ID	Vulnerability Description	Solution
Kernel	2.0	CVE-2018-6927	The futex_requeue function in kernel/futex.c in the Linux kernel before 4.14.15 might allow attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact by triggering a negative wake or requeue value.	Merge in package
linux_kernel	3.0	CVE-2018-5344	In the Linux kernel through 4.14.13, drivers/block/loop.c mishandles lo_release serialization, which allows attackers to cause a denial of service (__lock_acquire use-after-free) or possibly have unspecified other impact.	Merge in package