

Product name	Confidentiality level
B310s-22	CONFIDENTIAL
Product version	Total 14 pages
V4.0	

B310s-22 Firmware Release Notes

Prepared by	B310s-22 Team	Date	2016-09-17
Reviewed by	B310s-22 Team	Date	2016-09-17
Approved by	B310s-22 Team	Date	2016-09-17



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2015-2-6	1.0	FW 21.300.01.00.00	The 1 th Version	B310s-22 Team
2015-3-18	1.1	FW 21.300.05.00.00	The 2 th Version	B310s-22 Team
2015-3-30	1.2	FW 21.300.07.00.00	The 3 th Version	B310s-22 Team
2015-5-14	2.0	FW 21.311.03.00.00	The 4 th Version	B310s-22 Team
2015-6-27	2.1	FW 21.311.05.00.00	The 5 th Version	B310s-22 Team
2015-9-16	3.0	FW21.313.01.00.00	The 6 th Version	B310s-22 Team
2015-10-15	3.1	FW21.313.03.00.00	The 7 th Version	B310s-22 Team
2015-11-22	3.2	FW21.313.05.00.00	The 8 th Version	B310s-22 Team
2016-01-28	4.0	FW21.316.01.00.00	The 9 th Version	B310s-22 Team
2016-05-28	5.0	FW21.318.01.00.00	The 10 th Version	B310s-22 Team
2016-09-02	6.0	FW21.321.01.00.00	The 11 th Version	B310s-22 Team
2016-09-14	6.1	FW21.321.02.00.00	The 12 th Version	B310s-22 Team
2016-09-17	6.2	FW21.321.03.00.00	The 13 th Version	B310s-22 Team

Table of Contents

1	Main Features	4
2	Hardware.....	5
2.1	Version Description	5
2.2	Hardware Specifications	5
2.3	Improvements in the Previous Version	6
2.4	Known Limitations and Issues	7
3	Firmware	7
3.1	Version Description	7
3.2	Firmware Specifications	7
3.3	Improvement in the Previous Version	8
3.4	Known Limitations and Issues	9
4	WebUI.....	9
4.1	Version Description	9
4.2	WebUI/HiLink Specifications	9
4.3	Improvement in the Previous Version	9
4.4	Known Limitations and Issues	9
5	Software Vulnerabilities Fixes	9

B310s-22 Firmware Release Notes

Abbreviations	description

1 Main Features

The B310s-22 mainly supports the following features:

- LTE FDD (DL) data service of up to 150 Mbit/s
- LTE FDD (UL) data service of up to 50 Mbit/s
- LTE TDD (DL) data service of up to 112 Mbit/s
- LTE TDD (UL) data service of up to 10 Mbit/s
- DC-HSPA+ (DL) data service of up to 42 Mbit/s
- HSPA+ (DL) data service of up to 21.6 Mbit/s
- HSDPA (DL) data service of up to 14.4 Mbit/s
- HSUPA (UL) data service of up to 5.76 Mbit/s
- UMTS data service of up to 384 kbit/s
- EDGE data service of up to 236.8 kbit/s
- EDGE data service of download to 296 kbit/s
- GPRS data service of up to 85.6 kbit/s
- PS domain data service based on LTE/UMTS/GSM
- SMS based on CS/PS domain of GSM and UMTS, CS domain of LTE
- Wi-Fi
- Support for HUAWEI Mobile WiFi App
- Press and Play
- IPv6v4 /IPv4 dual stack
- Built-in DHCP Server, DNS RELAY and NAT
- Online software upgrade
- Traffic statistic
- LED indicators
- Built-in UMTS and WLAN high gain antenna LTE/GSM
- 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:	WL1B310FM03 (B310s-22)
Platform & Chipset:	Balong Hi6921 & AR 8035

2.2 Hardware Specifications

Item	Specifications	
Technical standard	WAN: LTE/ DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS/GSM	
	WLAN: IEEE 802.11b/g/n	
Operating frequency	LTE: B1/B3/B7/B8/B20/B38	
	HSPA+/HSPA/UMTS: B1/B8	
	EDGE/GPRS/GSM: 1900/1800/900/850 MHz	
	WLAN: 2.4 GHz	
Internal memory	512 MB Flash, 256 MB Memory	
Maximum transmitter power	UMTS: 24 (+1/-3) dBm	
	WLAN	802.11b: 16 dBm
		802.11g: 17 dBm
		802.11n: 17 dBm
Receiver sensitivity	UMTS: Confirm to 3GPP Requirements	
	WLAN 802.11b	-76 dBm@11 Mbit/s
		-82 dBm@1 Mbit/s
	WLAN 802.11g: -65 dBm@54 Mbit/s	
	WLAN 802.11n: -64 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: 1 RJ45, GE	
	FXS: 1 RJ11	
	SIM card interface: standard 6-pin SIM card interface	

Item	Specifications	
Indicators	Mode:	cyan: 4G mode blue: 3G mode yellow: 2G mode green: 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 White Steady On: 2.4G WiFi is opened Off: 2.4G WiFi is closed
	LAN	On/Off
	Power	On/Off
Button	Power switch, Reset switch, WPS switch	
Antenna	<ul style="list-style-type: none"> Built-in GSM/UMTS/LTE main diversity antenna Built-in GSM/UMTS/LTE diversity antenna Built-in WLAN antenna 	
Dimensions (D × W × H)	180 mm x126 mm x38mm	
Weight	about 226 g (Does not contain the power adapter)	
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:	21.321.03.00.00
Baseline information	BalongV700R110C30B321
OS	VxWorks 6.8+linux 3.4.5

3.2 Firmware Specifications

Item	Description
SMS	<ul style="list-style-type: none">• Writing/Sending/Receiving• Sending/Receiving extra-long messages• Storage: Up to 500 messages can be saved in the internal memory• New message prompt
Network connection setup	<ul style="list-style-type: none">• APN management: create, delete and edit.• Set up network connection
WLAN setup	<ul style="list-style-type: none">• 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
Firewall setup	<ul style="list-style-type: none">• Firewall Switch• LAN IP Filter• Virtual Server• DMZ Service

Item	Description
NAT setup	<ul style="list-style-type: none"> • CONE NAT • Symmetric NAT • ALG • VPN passthrough
DHCP setup	<ul style="list-style-type: none"> • DHCP server enabling and disabling • Address pool of the DHCP server setup • DHCP lease time setup
IPv6v4/IPv4 dual stack	DHCPv6/v4 server and client DNSv6/v4 server and client Display IPv6/v4 WAN address
Other	Network connection settings: <ul style="list-style-type: none"> • Automatic network selection and registration • Manual network selection and registration
	Network status display: signal, operator name, system mode, and so on.
	Selection of network connection types, for example: <ul style="list-style-type: none"> • Support LTE networks ON/OFF
	PIN management: activate/deactivate PIN, PIN lock, changing PIN, unblocking by using the PUK.
System requirement	<ul style="list-style-type: none"> • Windows XP SP3, Windows Vista SP1/SP2, Windows 7, Windows 8 (does not support Windows RT) • Mac OS X 10.6, 10.7 and 10.8 with latest upgrades • Your computer's hardware system should meet or exceed the recommended system requirements for the installed version of OS

3.3 Improvement in the Previous Version

Index	Case ID	Issue Description



3.4 Known Limitations and Issues

Index	Case ID	Issue Description

4 WebUI

4.1 Version Description

WebUI Version: 17.100.09.00.03

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/Module name	Version	CVE ID	Vulnerability Description	Solution
Portable UPnP SDK	LibUPnP 1.6.12	CVE-2012-5960	resolved	Refer:DTS2013012408852
Portable UPnP	LibUPnP 1.6.12	CVE-2012-5959	resolved	Refer:DTS2013012408852



SDK				
Portable UPnP SDK	LibUPnP 1.6.12	CVE-2012-5958	resolved	Refer:DTS2013012408852
Samba	3.0.37	CVE-2013-4475	Don't involve closing	Refer to the Samba website corresponding vulnerability, the problems in the Samba3.2.0 version, the current version is 3.0.37, refer : http://www.samba.org/samba/security/CVE-2013-4475
Samba	3.0.37	CVE-2013-4124	resolved	Refer:DTS2013101600954
Samba	3.0.37	CVE-2013-0454	resolved	Refer:DTS2013101600954
Samba	3.0.37	CVE-2013-0214	resolved	Refer:DTS2013101600954
Samba	3.0.37	CVE-2013-0213	resolved	Refer:DTS2013101600954
Samba	3.0.37	CVE-2012-1182	resolved	Refer:DTS2013101600954
Samba	3.0.37	CVE-2011-2724	Don't involve closing	Refer:DTS2013101600954
Samba	3.0.37	CVE-2011-2694	resolved	Refer:DTS2013101600954
Samba	3.0.37	CVE-2011-2522	resolved	Refer:DTS2013101600954
Samba	3.0.37	CVE-2011-1678	Don't involve closing	Refer:DTS2013101600954,/etc is a read-only file can not be tampered with
Samba	3.0.37	CVE-2011-0719	resolved	Refer:DTS2013101600954
Samba	3.0.37	CVE-2010-3069	resolved	Refer:DTS2013101600954
Samba	3.0.37	CVE-2010-2063	resolved	Refer:DTS2013101600954
Samba	3.0.37	CVE-2010-1642	resolved	Refer:DTS2013101600954
Samba	3.0.37	CVE-2010-1635	Don't involve closing	Refer:DTS2013101600954,there is no problem of output has been done to determine
Samba	3.0.37	CVE-2010-0547	Don't involve closing	Refer:DTS2013101600954,function problems do not exist without treatment
Samba	3.0.37	CVE-2012-6150	Don't involve closing	Refer to the Samba website corresponding vulnerability to explain the problem, in the 3.3.10, 3.4.3, 3.5.0 and later Later, the current version is 3.0.37, the specific reference : http://www.samba.org/samba/security/CVE-2012-6150

Samba	3.0.37	CVE-2013-4408	Don't involve closing	Refer:DTS2014011403455,the current version does not have this function, do not need to deal with
Openssl	0.98y	CVE-2014-3470	resolved	Refer:DTS2014060606113
Openssl	1.0.0a	CVE-2014-3470	resolved	Refer:DTS2014060606113
Openssl	1.0.1e	CVE-2014-3470	resolved	Refer:DTS2014060606113
Openssl	0.98y	CVE-2014-0224	resolved	Refer:DTS2014060606113
Openssl	1.0.0a	CVE-2014-0224	resolved	Refer:DTS2014060606113
Openssl	1.0.1e	CVE-2014-0224	resolved	Refer:DTS2014060606113
Openssl	0.98y	CVE-2014-0221	resolved	Refer:DTS2014060606113
Openssl	1.0.0a	CVE-2014-0221	resolved	Refer:DTS2014060606113
Openssl	1.0.1e	CVE-2014-0221	resolved	Refer:DTS2014060606113
Openssl	0.98y	CVE-2014-0198	resolved	Refer:DTS2014060606113
Openssl	1.0.0a	CVE-2014-0198	resolved	Refer:DTS2014060606113
Openssl	1.0.1e	CVE-2014-0198	resolved	Refer:DTS2014060606113
Openssl	0.98y	CVE-2014-0195	resolved	Refer:DTS2014060606113
Openssl	1.0.0a	CVE-2014-0195	resolved	Refer:DTS2014060606113
Openssl	1.0.1e	CVE-2014-0195	resolved	Refer:DTS2014060606113
Openssl	0.98y	CVE-2014-0076	resolved	Refer:DTS2014042811358
Openssl	0.98y	CVE-2014-3512	resolved	Refer:DTS2014082103995
Openssl	0.98y	CVE-2013-6450	resolved	Refer:DTS2014020804489
Samba	3.0.37	CVE-2013-4496	Don't involve closing	<p>CVE-2013-4496 vulnerability exists in the 3.4.0 version, the version is 3.0.37, without the need to merge. https://www.samba.org/samba/security/CVE-2013-4496</p> <p>Later, the current version is 3.0.37, the specific reference:http://www.samba.org/samba/security/CVE-2012-6150</p>
iptables	1.4.0	CVE-2012-2663	Don't involve closing	The influence of CVE-2012-2663 kernel version of the Linux kernel 2.6.x, the official website



				address access to modify the kernel code, the EUAP code of Linux kernel code, and do not call `iptables -m TCP --syn` command parameter, so no need to merge. Specific reference: http://git.kernel.org/cgit/linux/kernel/git/davem/net-next.git/commit/?id=fd5af0daf8019cec2396cdef8fb042d80fe71fa
CUPS	1.6.1	CVE-2014-2856	resolved	Refer:DTS2014042801913
Openssl	0.98y	CVE-2010-5298	resolved	Refer:DTS2014042903164
Openssl	1.0.1e	5846638	resolved	1.0.0a to see the vulnerability to introduce and explain the http://www.openssl.org/news/secadv_20140605.txt Synchronization update vulnerability, see CVE-2014-0224,CVE-2014-0221,CVE-2014-0195,CVE-2014-0198,CVE-2010-5298,CVE-2014-3470,CVE-2014-0076
Openssl	1.0.1e	CVE-2014-3505	resolved	Refer:DTS2014082103995
Openssl	1.0.1e	CVE-2014-3506	resolved	Refer:DTS2014082103995
Openssl	1.0.1e	CVE-2014-3507	resolved	Refer:DTS2014082103995
Openssl	1.0.1e	CVE-2014-3508	resolved	Refer:DTS2014082103995
Openssl	1.0.1e	CVE-2014-3510	resolved	Refer:DTS2014082103995
Openssl	1.0.1e	CVE-2014-5139	resolved	Refer:DTS2014082103995
Openssl	1.0.1e	CVE-2014-3512	resolved	Refer:DTS2014082103995
Openssl	1.0.1e	CVE-2014-3511	resolved	Refer:DTS2014082103995
Openssl	1.0.1e	CVE-2014-3513	resolved	Refer:DTS2014101702663
Openssl	1.0.1e	CVE-2014-3566	resolved	Refer:DTS2014101702663
Openssl	1.0.1e	CVE-2014-3567	resolved	Refer:DTS2014101702663
Openssl	1.0.1e	CVE-2014-3568	resolved	Refer:DTS2014101702663
Openssl	1.0.1a	CVE-2014-3513	resolved	Refer:DTS2014101702663
Openssl	1.0.1a	CVE-2014-3566	resolved	Refer:DTS2014101702663



Openssl	1.0.1a	CVE-2014-3567	resolved	Refer:DTS2014101702663
Openssl	1.0.1a	CVE-2014-3568	resolved	Refer:DTS2014101702663
		CVE-2014-3568	resolved	Refer:DTS2014101702663
		CVE-2014-3567	resolved	Refer:DTS2014101702663
		CVE-2014-3566	resolved	Refer:DTS2014101702663
		CVE-2014-3513	resolved	Refer:DTS2014101702663
		CVE-2014-2851	resolved	Refer:DTS2015021307041
		CVE-2013-1763	resolved	Refer:DTS2015021307041
		CVE-2014-4943	resolved	Refer:DTS2015021307041
Samba	3.0.37	CVE-2015-5252	resolved	Refer: DTS2016011910731
linux kernel	3.4.5	CVE-2015-1805	resolved	Refer: DTS2016032907086
Android	4.4_r1	CVE-2016-0774	resolved	Refer: DTS2016042909004
		CVE-2016-2438	resolved	Refer: DTS2016042909004
Openssl	1.0.1a	CVE-2016-2105	resolved	Refer: DTS2016051206645
		CVE-2016-2106	resolved	Refer: DTS2016051206645
		CVE-2016-2107	resolved	Refer: DTS2016051206645
		CVE-2016-2108	resolved	Refer: DTS2016051206645
		CVE-2016-2109	resolved	Refer: DTS2016051206645
		CVE-2016-2176	resolved	Refer: DTS2016051206645
Wifi		CVE-2016-0801	resolved	Refer: DTS2016031502450
		CVE-2016-0802	resolved	Refer: DTS2016031502450
Openssl		CVE-2015-8816	resolved	Refer: DTS2016082503595
		CVE-2016-0723	resolved	Refer: DTS2016082503595
		CVE-2016-3757	resolved	Refer: DTS2016082503595
		CVE-2016-2842	resolved	Refer: DTS2016071304872
		CVE-2015-2686	resolved	Refer: DTS2016071304872
		CVE-2016-3841	resolved	Refer: DTS2016071304872
		CVE-2016-4482	resolved	Refer: DTS2016071304872



Iptables		CVE-2014-9529	resolved	Refer: DTS2016080404468
		CVE-2015-5364	resolved	Refer: DTS2016080404468
		CVE-2016-4470	resolved	Refer: DTS2016080404468
		CVE-2016-4998	resolved	Refer: DTS2016080404468