

Product name	Confidentiality level
B311-221	CONFIDENTIAL
Product version	Total 10 pages
V2.0	

HUAWEI B311-221 Firmware Release Notes

V2.0

Prepared by	B311-221 Team	Date	2019-08-01
Reviewed by	B311-221 Team	Date	2019-08-01
Approved by	B311-221 Team	Date	2019-08-01



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2019-06-25	1.0	FW B311-221 10.0.1.1(H187SP1C983)	The First Version	B311-221 Team
2019-08-01	2.0	FW B311-221 10.0.1.1(H187SP60C983)	The Second Version	B311-221 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
4	Web UI	8
4.1	Version Description	8
4.2	Web UI Specifications	8
4.3	Known Limitations and Issues	8
5	Software Vulnerabilities Fixes	8



HUAWEI B311-221 Firmware Release Notes V2.0

Abbreviations	Description

1 Main Features

The B311-221 supports the following standards:

- 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
- SMS based on CS/PS domain of LTE
- Wi-Fi
- Support for HUAWEI HiLinkApp
- IPv4v6 Dual stack
- Built-in DHCP Server, DNS RELAY and NAT
- Traffic statistic
- LED indicators
- Built-in LTE and WLAN antenna
- Windows 7, Windows 8, Windows 8.1, Windows 10 (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:	WL5B311M Ver.A
Platform & Chipset:	Balong V700R11C70B187

2.2 Hardware Specifications

Item	Specifications
Technical standard	WAN: LTE
	WLAN: IEEE 802.11b/g/n
Operating frequency	LTE B1/3/7/8/20/38 UMTS B1/8 GSM B2/3/5/8
	WLAN: 2.4 GHz
Internal memory	512 MB Flash, 256 MB DDR



Item	Specifications	
Maximum transmitter power	LTE: 24 (+1/-3) dBm	
	WLAN	802.11b: 13 (+/-2) dBm
		802.11g: 13 (+/-2) dBm
		802.11n: 13 (+/-2) dBm
Receiver sensitivity	LTE: 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	LAN: 1 RJ45,GE FXS:1 RJ11	
	SIM card interface: standard 6-pin SIM card interface	
Indicators	Mode:	cyan: LTE 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	



Item	Specifications
Antenna	• Built-in LTE main antenna • Built-in LTE diversity antenna • Built-in WLAN antenna
Dimensions (D × W × H)	181 mm x 126 mm x 36 mm
Weight	about 500 g (Does not contain the power adapter)
Temperature	Operating: 0°C to +40°C
	Storage: -20°C to +70°C
Humidity	5% to 95% (non-condensing)

2.3 Improvements in the Previous Version

Index	Case ID	Issue Description
Hardware Version		WL5B311M Ver.A
Previous Version	Hardware	Pre-verification Samples

2.4 Known Limitations and Issues

Index	Case ID	Issue Description
NA		

3 Firmware

3.1 Version Description

Firmware Version: B311-221 10.0.1.1(H187SP60C983)

Baseline information Balong V700R11C70B187

3.2 Firmware Specifications

We have add following Specifications in this version

Item	Description
SMS	• Writing/Sending/Receiving • Sending/Receiving extra-long messages • Storage: Up to 500 messages can be saved in the internal memory • New message prompt



Item	Description
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 • Guest Wi-Fi • Hilink
Firewall setup	• Firewall Switch • LAN IP Filter • Virtual Server • DMZ Service
NAT setup	• CONE NAT • Symmetric NAT • ALG • VPN
DHCP setup	• DHCP server enabling and disabling • Address pool of the DHCP server setup • DHCP lease time setup
IPv4v6 Dou stack	• DHCPv4v6 server and client • DNSv4 v6server and client • Display IPv4v6 WAN address
System requirement	• 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



4 Web UI

4.1 Version Description

Web UI Version: WEBUI 10.0.1.1(W2SP5C03)

4.2 Web UI Specifications

Case ID	Issue Description
---------	-------------------

4.3 Known Limitations and Issues

Index	Case ID	Issue Description
	NA	

5 Software Vulnerabilities Fixes

Software/Module name	Version	CVE ID	Vulnerability Description	Impact Description
<i>Kernel</i>	<i>3.10.100</i>	<i>CVE-1999-0524</i>	<i>ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.</i>	<i>https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-1999-0524</i>
<i>Kernel</i>	<i>3.10.100</i>	<i>CVE-2017-6951</i>	<i>The keyring_search_aux function in security/keys/keyring.c in the Linux kernel through 3.14.79 allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a</i>	<i>https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2017-6951</i>



			<i>request_key system call for the "dead" type.</i>	
<i>Kernel</i>	<i>3.10.100</i>	<i>CVE-2019-11190</i>	<i>The Linux kernel before 4.8 allows local users to bypass ASLR on setuid programs (such as /bin/su) because install_exe_c_creds() is called too late in load_elf_binary() in fs/binfmt_elf.c, and thus the ptrace_may_access() check has a race condition when reading /proc/pid/stat.</i>	<i>https://git.kernel.org/pub/scm/linux/kernel/git/stable/stable-queue.git/commit/?id=a5b5352558f6808db0589644ea5401b3e3148a0d</i>
<i>Kernel</i>	<i>3.10.100</i>	<i>CVE-2017-5972</i>	<i>The TCP stack in the Linux kernel 3.x does not properly implement a SYN cookie protection mechanism for the case of a fast network connection, which allows remote attackers to cause a denial of service (CPU consumpti</i>	<i>https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2017-5972</i>



			on) by sending many TCP SYN packets, as demonstrated by an attack against the kernel-3.10.0 package in CentOS Linux 7. NOTE: third parties have been unable to discern any relationship between the GitHub Engineering finding and the Trigemini.c attack code.	
Kernel	3.10.100	CVE-2018-9517	In pppol2tp_connect, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID:	https://www.cvedetails.com/cve-details.php?t=1&cve_id=CVE-2018-9517



			A-3815993 1.	