

Product name	Confidentiality level
B311-221	CONFIDENTIAL
Product version	Total 11pages
V1.8	

HUAWEI B311-221 Firmware Release Notes

V1.8

Prepared by	B311-221 Team	Date	2020-03-12
Reviewed by	B311-221 Team	Date	2020-03-12
Approved by	B311-221 Team	Date	2020-03-12



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2019-10-26	1.7	FW: B311-221 RTOS 10.0.2.1(H690SP1C00 WEBUI : WEBUI 10.0.2.1(W2SP1C03)	The 7 st Version	B311-221 Team
2020-03-12	1.8	FW: B311-221 RTOS 10.0.2.1(H690SP3C00 WEBUI : WEBUI 10.0.2.1(W2SP2C03)	The 8 st 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 V1.8

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 smartHome App
- 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 V700R11C70B190

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 10.0.2.1(H690SP3C00)

Baseline information Balong V700R11C70B190

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 10.0.2.1(W2SP2C03)

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
expat	2.2.6	CVE-2018-20843	In libexpat in Expat before 2.2.7, XML input including XML names that contain a large number of colons could make the XML parser consume a high amount of RAM and CPU resources while processing (enough to be usable for denial-of-service attacks).	https://github.com/libexpat/libexpat/pull/262/commits/11f8838b99ea0a6f0b76f9760c43704d00c4ff6
Kernel	4.4	CVE-2019-12456	An issue was discovered in the MPT3COMMAND case in _ctl_ioctl_main in drivers/scsi/mpt3sas/mpt3sas_ctl.c in the Linux kernel through 5.1.5. It allows local users to cause a denial of service or possibly have unspecified other impact by changing the value of ioc_number between two kernel reads of that value, aka a "double fetch" vulnerability	https://git.kernel.org/pub/scm/linux/kernel/git/mkp/scsi.git/commit/?h=5.3/scsi-queue&id=86e5aca7fa2927060839f3e3b40c8bd65a7e8d1e
Kernel	4.4	CVE-2019-11478	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service.	https://github.com/NetfliX/security-bulletins/blob/master/advisories/third-party/2019-001.md
Kernel	4.4	CVE-2018-9422	In get_futex_key of futex.c, there is a use-after-free due to improper locking. This could lead to local escalation of privilege with no additional privileges needed. User interaction is not needed	https://source.android.com/security/bulletin/2018-07-01



			for exploitation	
Kernel	4.4	CVE-2019-13272	In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic).	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6994eefb0053799d2e07cd140df6c2ea106c41ee
Kernel	4.4	CVE-2019-15220	An issue was discovered in the Linux kernel before 5.2.1. There is a use-after-free caused by a malicious USB device in the drivers/net/wireless/intersil/p54/p54usb.c driver.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6e41e2257f1094acc37618bf6c856115374c6922
Kernel	4.4	CVE-2019-15219	An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the drivers/usb/misc/sisusbvga/sisusb.c driver.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=9a5729f68d3a82786aea110b1bfe610be318f80a
Kernel	4.4	CVE-2019-15221	An issue was discovered in the Linux kernel before 5.1.17. There is a NULL pointer dereference caused by a malicious USB device in the sound/usb/line6/pcm.c driver.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3450121997ce872eb7f1248417225827ea249710
Kernel	4.4	CVE-2019-15217	An issue was discovered in the Linux kernel before 5.2.3. There is a NULL pointer dereference caused by a malicious USB device in the drivers/media/usb/zr364xx/zr364xx.c driver.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=5d2e73a5f80a5b5aff3caf1ec6d39b5b3f54b26e
Kernel	4.4	CVE-2019-12819	An issue was discovered in the Linux kernel before 5.0. The function __mdiobus_register() in drivers/net/phy/mdio_bus.c calls put_device(), which will trigger a fixed_mdio_bus_init use-after-free. This will cause a denial of service.	https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6ff7b060535e87c2ae14dd8548512abfdda528fb
Kernel	4.4	CVE-2019-15214	An issue was discovered in the Linux kernel before 5.0.10. There is a use-after-free in the sound subsystem because card disconnection causes certain data structures to be deleted too early. This is related to sound/core/init.c and sound/core/info.c.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8c2f870890fd28e023b0fcf49dcee333f2c8bad7
Kernel	4.4	CVE-2019-15216	An issue was discovered in the Linux kernel before 5.0.14. There is a NULL pointer dereference caused by a malicious USB device in the drivers/usb/misc/yurex.c driver.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ef61eb43ada6c1d6b94668f0f514e4c268093ff3
Kernel	4.4	CVE-2019-15666	An issue was discovered in the Linux kernel before 5.0.19. There is an out-of-bounds array access in __xfrm_policy_unlink, which will cause	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b805d78d300bcf2c83d6df7da0c818b0fee41427



			denial of service, because verify_newpolicy_info in net/xfrm/xfrm_user.c mishandles directory validation.	
Kernel	4.4	CVE-2019-3846	A flaw that allowed an attacker to corrupt memory and possibly escalate privileges was found in the mwifex kernel module while connecting to a malicious wireless network.	https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/KLGWJKLMTBBB53D5QLS4HOY2EH246WBE/FEDORA-FEDORA-2019-7ec378191e
Kernel	4.4	CVE-2016-0728	The join_session_keyring function in security/keys/process_keys.c in the Linux kernel before 4.4.1 mishandles object references in a certain error case, which allows local users to gain privileges or cause a denial of service (integer overflow and use-after-free) via crafted keyctl commands.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=23567fd052a9abb6d67fe8e7a9ccdd9800a540f2 CONFIRM
Kernel	4.4	CVE-2019-15213	An issue was discovered in the Linux kernel before 5.2.3. There is a use-after-free caused by a malicious USB device in the drivers/media/usb/dvb-usb/dvb-usb-init.c driver.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6cf97230cd5f36b7665099083272595c55d72be7
Kernel	4.4	CVE-2019-15212	An issue was discovered in the Linux kernel before 5.1.8. There is a double-free caused by a malicious USB device in the drivers/usb/misc/rio500.c driver.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3864d33943b4a76c6e64616280e98d2410b1190f
Kernel	4.4	CVE-2019-15215	An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the drivers/media/usb/cpia2/cpia2_usb.c driver.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=eff73de2b1600ad8230692f00bc0ab49b166512a
Kernel	4.4	CVE-2019-15218	An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the drivers/media/usb/siano/smsusb.c driver.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=31e0456de5be379b10fea0fa94a681057114a96e
Kernel	4.4	CVE-2019-10142	A flaw was found in the Linux kernel's freescale hypervisor manager implementation, kernel versions 5.0.x up to, excluding 5.0.17. A parameter passed to an ioctl was incorrectly validated and used in size calculations for the page size calculation. An attacker can use this flaw to crash the system, corrupt memory, or create other adverse security affects.	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10142
Kernel	4.4	CVE-2019-2054	In the seccomp implementation prior to kernel version 4.8, there is a possible seccomp bypass due to seccomp policies that allow the use of ptrace. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	http://packetstormsecurity.com/files/153799/Kernel-Live-Patch-Security-Notice-LSN-0053-1.html



<i>Kernel</i>	<i>4.4</i>	<i>CVE-2019-15211</i>	<i>An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the drivers/media/v4l2-core/v4l2-dev.c driver because drivers/media/radio/radio-raremono.c does not properly allocate memory.</i>	<i>https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c666355e60ddb4748ead3bdd983e3f7f2224aaf0</i>