

B311s-220 8.0.1.9(H183SP2C11)

Release Notes

Prepared by	B311s-220 Team	Date	2019-06-19
Reviewed by	B311s-220 Team	Date	2019-06-19
Approved by	B311s-220 Team	Date	2019-06-19



Huawei Technologies Co., Ltd.

All rights reserved

Table of Contents

1.	Main Features	3
2.	Hardware	3
	2.1 Version Description	3
	2.2 Hardware Specifications	3
3.	Firmware.....	5
	3.1 Version Description	5
	3.2 Improvement in the Previous Version.....	5
	3.3 Known Limitations and Issues	5
4.	Software Vulnerabilities Fixes	5

1. Main Features

The B311s-220 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:	WL1B311M
Platform & Chipset:	Balong V700R11C70B182

2.2 Hardware Specifications

Item	Specifications
Technical standard	WAN: LTE
	WLAN: IEEE 802.11b/g/n

Item	Specifications	
Operating frequency	LTE B1/3/7/8/20	
	UMTS B1/8	
	GSM B2/3/5/8	
	WLAN: 2.4 GHz	
Internal memory	512 MB Flash,256 MB DDR	
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

Item	Specifications	
	LAN	On/Off
	Power	On/Off
Button	Power switch, Reset switch, WPS switch	
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: -40°C to +70°C	
Humidity	5% to 95% (non-condensing)	

3. Firmware

3.1 Version Description

Firmware Version:	8.0.1.9(H183SP2C11)
WEBUI Version:	WEBUI 8.0.1.31(W2SP2C11)
Baseline information	Balong V700R11C70B182

3.2 Improvement in the Previous Version

Index	Description
1	REQ.011; Add the other language translation WEBSDK-E-034-36-CUS:IMEISV+1

3.3 Known Limitations and Issues

Index	Issue Description
NA	

4. Software Vulnerabilities Fixes

Software/Module name	Version	CVE ID	Vulnerability Description	Impact Description
		CVE-2017-9074	The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider	

			that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls.	
		CVE-2017-7487	The ipxif_ioctl function in net/ipx/af_ipx.c in the Linux kernel through 4.11.1 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a failed SIOCGIFADDR ioctl call for an IPX interface.	
		CVE-2017-9242	The __ip6_append_data function in net/ipv6/ip6_output.c in the Linux kernel through 4.11.3 is too late in checking whether an overwrite of an skb data structure may occur, which allows local users to cause a denial of service (system crash) via crafted system calls.	
		CVE-2017-13216	Google Android Bugs Let Remote Users Obtain Sensitive Information, Deny Service, and Execute Arbitrary Code	
		CVE-2017-16535	The usb_get_bos_descriptor function in drivers/usb/core/config.c in the Linux kernel before 4.13.10 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.	
		CVE-2017-16531	drivers/usb/core/config.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device, related to the USB_DT_INTERFACE_ASSOCIATION descriptor	
		CVE-2017-15274	security/keys/keyctl.c in the Linux kernel before 4.11.5 does not consider the case of a NULL payload in conjunction with a nonzero length value, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted add_key or keyctl system call, a different vulnerability than CVE-2017-12192.	
		CVE-2017-12192	The keyctl_read_key function in security/keys/keyctl.c in the Key Management subcomponent in the Linux kernel before 4.13.5 does not properly consider that a key may be possessed but negatively instantiated, which allows local users to cause a denial of service (OOPS and system crash) via a crafted KEYCTL_READ operation.	
		CVE-2017-1000111	Linux kernel: heap out-of-bounds in AF_PACKET sockets. This new issue is analogous to previously disclosed CVE-2016-8655. In both cases, a socket option that changes socket state may race with safety checks in packet_set_ring. Previously with PACKET_VERSION. This time with PACKET_RESERVE. The solution is similar: lock the socket for the update. This issue may be exploitable, we did not investigate further. As this issue affects PF_PACKET sockets, it requires CAP_NET_RAW in the process namespace. But note that with user namespaces enabled, any process	

			can create a namespace in which it has CAP_NET_RAW.	
		CVE-2017-15649	net/packet/af_packet.c in the Linux kernel before 4.13.6 allows local users to gain privileges via crafted system calls that trigger mishandling of packet_fanout data structures, because of a race condition (involving fanout_add and packet_do_bind) that leads to a use-after-free, a different vulnerability than CVE-2017-6346.	
		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	
		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.	
		CVE-2016-10044	The aio_mount function in fs/aio.c in the Linux kernel before 4.7.7 does not properly restrict execute access, which makes it easier for local users to bypass intended SELinux W^X policy restrictions, and consequently gain privileges, via an io_setup system call.	
		CVE-2017-0427	An elevation of privilege vulnerability in the kernel file system could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31495866.	
		CVE-2016-6753	An information disclosure vulnerability in kernel components, including the process-grouping subsystem and the networking subsystem, in Android before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Android ID: A-30149174.	
		CVE-2017-18255	The perf_cpu_time_max_percent_handler function in kernel/events/core.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow) or possibly have unspecified other impact via a large value, as demonstrated by an incorrect sample-rate calculation.	
		CVE-2018-1000199	An address corruption flaw was discovered in the Linux kernel built with hardware breakpoint (CONFIG_HAVE_HW_BREAKPOINT) support. While modifying a h/w breakpoint via 'modify_user_hw_breakpoint' routine, an unprivileged user/process could use this flaw to crash the system kernel resulting in DoS OR to potentially escalate privileges on a the system.	
		CVE-2018-9389	This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be	



			provided	
		CVE-2018-10124	The kill_something_info function in kernel/signal.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service via an INT_MIN argument.	