

Product name	Confidentiality level
B311s-220	CONFIDENTIAL
Product version	Total 13pages
V1.14	

HUAWEI B311s-220 Firmware Release Notes

V1.14

Prepared by	B311s-220 Team	Date	2019-06-03
Reviewed by	B311s-220 Team	Date	2019-06-03
Approved by	B311s-220 Team	Date	2019-06-03



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2017-11-13	1.0	FW B311s-220 6.0.1.1(H90SP1C00) WEBUI 6.0.1.3(W2SP1C03)	The 1 st Version	B311s-220 Team
2017-12-7	1.1	FW B311s-220 6.0.1.3(H100SP4C00) WEBUI 6.0.1.5(W2SP1C03)	TR4 Test Version	B311s-220 Team
2018-1-8	1.2	FW B311s-220 8.0.1.1(H130SP1C00) WEBUI 8.0.1.1(W2SP1C03)	Pre-TR4A Test Version	B311s-220 Team
2018-1-19	1.3	FW B311s-220 8.0.1.1(H150SP1C00) WEBUI 8.0.1.3(W2SP1C03)	TR4A Test Version	B311s-220 Team
2018-2-24	1.4	FW B311s-220 8.0.1.9(H160SP1C00) WEBUI 8.0.1.7(W2SP1C03)	TR5 Test Version	B311s-220 Team
2018-3-14	1.5	FW B311s-220 8.0.1.1(H180SP1C00) WEBUI 8.0.1.9(W2SP1C03)	TR6 Test Version	B311s-220 Team
2018-3-20	1.6	FW B311s-220 8.0.1.5(H180SP1C00) WEBUI 8.0.1.11(W2SP1C03)	TR6 Test Version	B311s-220 Team
2018-3-22	1.7	FW B311s-220 8.0.1.7(H180SP1C00) WEBUI 8.0.1.13(W2SP1C03)	TR6 Test Version	B311s-220 Team
2018-7-20	1.8	FW B311s-220 8.0.1.1(H182SP1C00) WEBUI 8.0.1.17(W2SP1C03)	MR1 Test Version	B311s-220 Team
2018-7-24	1.9	FW B311s-220 8.0.1.3(H182SP1C00) WEBUI 8.0.1.19(W2SP1C03)	MR1-1 Test Version	B311s-220 Team



2018-12-14	1.10	FW B311s-220 8.0.1.9(H183SP1C00) WEBUI 8.0.1.30 (W2SP1C03)	MR2 Test Version	B311s-220 Team
2019-1-12	1.11	FW B311s-220 8.0.1.9(H183SP3C00) WEBUI 8.0.1.31(W2SP1C03)	MR2-1 Test Version	B311s-220 Team
2019-3-11	1.12	FW B311s-220 8.0.1.1(H185SP3C00) WEBUI 8.0.1.32(W2SP1C03)	MR3-1 Test Version	B311s-220 Team
2019-3-27	1.13	FW B311s-220 8.0.1.1(H186SP5C00) WEBUI 8.0.1.32(W2SP3C03)	MR3-2 Test Version	B311s-220 Team
2019-6-3	1.13	FW B311s-220 10.0.1.1(H187SP11C00) WEBUI 10.0.1.1(W2SP3C03)	MR4 Test Version	B311s-220 Team

Table of Contents

1	Main Features	5
2	Hardware.....	5
2.1	Version Description	5
2.2	Hardware Specifications	5
2.3	Improvements in the Previous Version	7
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
4	Web UI	9
4.1	Version Description	9
4.2	Web UI Specifications	9
4.3	Known Limitations and Issues	9
5	Software Vulnerabilities Fixes.....	10

HUAWEI B311s-220 Firmware Release Notes V1.14

Abbreviations	Description

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 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 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:WLAN 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: -40°C to +70°C
Humidity	5% to 95% (non-condensing)

2.3 Improvements in the Previous Version

Index	Case ID	Issue Description
Hardware Version		WL1B311M
Previous Version	Hardware	Pre-verification Samples
NA		

2.4 Known Limitations and Issues

Index	Case ID	Issue Description
NA		

3 Firmware

3.1 Version Description

Firmware Version: B311s-220 10.0.1.1(H187SP11C00)

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 of the B315s-938. • New message prompt
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
1	DTS2019052708853	【随卡匹配】【P711/722/750 随卡匹配方案共性问题】C 版本号的 plmn_list 中设置了 PLMN 的限制名单,插入限制名单中 PLMN 的 SIM 卡后,无法正常加载 PLMN 对应的 NV。预期结果:插入白名单包含的 PLMN 对应的 SIM 卡后,能够正常加载对应的 NV。影响随卡特性 NV 定制 C 版本限制 plmnlist 使用。
2	DTS2019051701115	【在线升级支持 HTTPS】【B311s-220 8.0.1.1(H186SP5C00) 必现】B311s-220&As-853 产品规格明确在线升级应该支持 HTTPS,而实际产品配置默认支持 HTTP,与单板规格严重不符,请修改。
3	DTS2019042502797	【安全】【开源声明_必现】开源声明中需要更新 ebtables、iproute2、iptables、radvd、BusyBox 组件版本号,需要删除 BusyBox 1.9.1 组件描述。(和开发马文斌确认 8015 分支出来以后主线开源声明版本更新导致该问题,所以 8015 以及以前的分支不涉及该问题)
4	DTS2019041006481	【同步至 B311s-220 产品】【EMUI8.0】【新需求】当前 WIFI 密码容易被破解,需要整改(从默认 8 位密码整改为 11 位数字+大写字母随机字符串)。

4 Web UI

4.1 Version Description

Web UI Version: WEBUI 10.0.1.1(W2SP3C03)

4.2 Web UI Specifications

Case ID	Issue Description
1	【WiFi_高概率】2.4G 和 5G WiFi 任意关闭一个,然后到“更多 WLAN 设置”页面修改“带宽”“信道”及“最大接入数”都提示失败,配置不成功。
2	【WEBUI 8.0.1.32(W0SP1C03)_域名过滤_必现】进入安全-域名过滤页面,切换域名过滤模式为“白名单”,无法切换成功,影响功能使用(新引入,8013 不涉及)
3	【EMUI8.0_VOIP 特性_必现】8.0 UI VOIP PASSWORD 栏设置包含 \?; 等的特殊字符,设置失败,提示无法设置,UI 对特殊字符有限制。导致产品定制包含特殊字符密码时无法定制(对比 5.0UI, PASSWORD 栏设置包含特殊字符(\?;) 的密码,可以设置保存成功)
4	【共性问题】【B316-855 8.0.1.1(H191SP5C233)_短信_概率重现】在 WEBUI 短信界面,自发自收短信 15 条左右,删除其他一条,部分消息不显示。

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
		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.	