

Product name	Confidentiality level
B311As-853	CONFIDENTIAL
Product version	Total 10 pages
V1.0	

B311As-853 Firmware Release Notes

V1.0

Prepared by	B311As-853 Team	Date	2019-6-3
Reviewed by	B311As-853 Team	Date	2019-6-3
Approved by	B311As-853 Team	Date	2019-6-3



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2017-12-5	1.0	FW:6.0.1.3(H100SP4C00) WEBUI 6.0.1.5(W2SP1C03)	The 1 st Version	B311As-853 Team
2018-1-19	2.0	FW:6.0.1.3(H100SP4C00) WEBUI 6.0.1.5(W2SP1C03)	The 2 nd Version	B311As-853 Team
2018-1-27	3.0	FW:8.0.1.1(H150SP4C00) WEBUI 8.0.1.3(W2SP3C03)	The 3 rd Version	B311As-853 Team
2018-3-12	4.0	FW:8.0.1.5(H180SP1C00) WEBUI 8.0.1.13(W2SP1C03)	The 4 th Version	B311As-853 Team
2018-7-20	5.0	FW:8.0.1.1(H182SP1C00) WEBUI 8.0.1.17(W2SP1C03)	The 5 th Version	B311As-853 Team
2018-8-23	6.0	FW: 8.0.1.7(H182SP1C00) WEBUI 8.0.1.23(W2SP1C03)	The 6 th Version	B311As-853 Team
2018-12-13	7.0	FW: 8.0.1.9(H183SP1C00) WEBUI 8.0.1.30(W2SP1C03)	The 7 th Version	B311As-853 Team
2019-1-11	8.0	FW: 8.0.1.9(H183SP3C00) WEBUI 8.0.1.31(W2SP1C03)	The 8 th Version	B311As-853 Team
2019-3-27	9.0	FW: 8.0.1.1(H186SP5C00) WEBUI 8.0.1.32(W2SP3C03)	The 9 th Version	B311As-853 Team
2019-6-3	10.0	FW: 10.0.1.1(H187SP11C00) WEBUI 10.0.1.1(W2SP3C03)	The 10 th Version	B311As-853 Team

Table of Contents

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



1 Main Features

The B311As-853 supports the following standards:

- LTE FDD: DL 150Mbps, UL 50Mbps
- LTE TDD: DL 110Mbps, UL 11Mbps
- TDS-CDMA:DL 2.8Mbps,UL 2.2Mbps
- DC-HSPA+: DL 42 Mbps, UL 5.76 Mbps
- HSPA+: DL 21 Mbps (64QAM), UL 5.76 Mbps
- HSPA: DL 14.4 Mbps, UL 5.76 Mbps
- WCDMA PS: DL 384 Kbps, UL 384 Kbps
- WIFI 2.4G:802.11b/g/n,2*2MIMO 300Mbps
- Equalizer and receive diversity

2 Hardware

2.1 Version Description

Hardware Version:	WL2B311M Ver.A
Platform & Chipset:	Balong Hi6921 V7R11



2.2 Hardware Specifications

Item	Specifications	
Technical Standard	LTE	3GPP R9
	WCDMA	3GPP R8
	TDS-CDMA	3GPP R9
Operating Frequency	LTE	Band1,Band3,Band5,Band8 ,Band26,Band28,Band34,B and38,Band39,Band40,Ban d41(Band41: 2545~2655)
	TDS	Band34,Band39
	UMTS	Band1,Band5,Band8
Memory	Flash 512MB/DDR 256MB	
WLAN Rate	802.11b: 1/2/5.5/11 Mbit/s	
	802.11g: 6/9/12/18/24/36/48/54 Mbit/s, compatible 802.11b rate	
	8.2.11n:compatible 802.11b rate and 802.11g rate	
	HT20: Support MCS0–MCS7; Up to 65 Mbit/s. Support MCS8–MCS15; Up to 130 Mbit/s.	
	HT40: Support MCS0–MCS7; Up to 135 Mbit/s. Support MCS8–MCS15; Up to 270 Mbit/s.	
External Interfaces	LED: Power/MODE/WLAN/LAN/SIGNAL (3bar)	
	Ethernet port:1 GE	
	SIM/USIM card: 1 2FF	
	SMA:1	
Keys	1 Power,1 Reset,1 Wps	
Battery	NA	
Ambient 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	WL2B311M Ver.A	
Previous Hardware Version	Pre-verification Samples	

2.4 Known Limitations and Issues

Index	Case ID	Issue Description
NA		



3 Firmware

3.1 Version Description

Firmware Version:	10.0.1.1(H187SP11C00)
Baseline information	Balong Hi6921 V7R11
OS	Linux 3.10.100

3.2 Firmware Specifications

Item	Specifications
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



Item	Specifications
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		

3.4 Known Limitations and Issues

Index	Case ID	Issue Description

4 WebUI/HiLink

4.1 Version Description

WebUI/HiLink Version: **WEBUI 10.0.1.1(W2SP3C03)**

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
1	Unrealized Features	DBDC is disabled

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	

[带格式表格](#)



			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.	