

Product name	Confidentiality level
B310As-938	CONFIDENTIAL
Product version	Total 9 pages
V1.2	

HUAWEI B310As-938 Firmware Release

Notes V1.2

Prepared by	B310As-938 Team	Date	2017-05-22
Reviewed by	B310As-938 Team	Date	2017-05-22
Approved by	B310As-938 Team	Date	2017-05-22



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2017-05-22	1.1	FW 11.326.01.00.1342 WebUI 21.100.33.00.03	The 1 st Version	B310As-938 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
	We have add following Specifications in this version	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 B310As-938 Firmware Release Notes V1.2

Abbreviations	Description

1 Main Features

The B310As-938 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 Mobile WiFi App
- Press and Play
- IPv4v6 Dou stack
- Built-in DHCP Server, DNS RELAY and NAT
- Traffic statistic
- LED indicators
- Built-in LTE and WLAN high gain antenna
- Windows XP SP3, Windows Vista SP1/SP2, Windows 7, Windows 8, Windows 8.1 (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:	WL2B310M01
Platform & Chipset:	ATPV2,Balong

2.2 Hardware Specifications

Item	Specifications
Technical standard	WAN: LTE
	WLAN: IEEE 802.11b/g/n
Operating frequency	LTE: B3/B28/B41
	HSPA+/HSPA/UMTS: B1(2100) /B8(900) MHz
	WLAN: 2.4 GHz
Internal memory	512 MB Flash,256 MB Memory



Item	Specifications	
Maximum transmitter power	LTE: 24 (+1/-3) dBm	
	WLAN	802.11b: 16 (+/-3) dBm
		802.11g: 17 (+/-3) dBm
		802.11n: 17 (+/-3) 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	
	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	<ul style="list-style-type: none">• Built-in LTE main antenna• Built-in LTE diversity antenna• Built-in WLAN antenna
Dimensions (D × W × H)	180 mm x126 mm x38mm
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		WL2B310M01
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:	11.326.01.00.1342
Baseline information	Balong V700R11C30B326

3.2 Firmware Specifications

We have add following Specifications in this version




Item	Description
SMS	<ul style="list-style-type: none">• Writing/Sending/Receiving• Sending/Receiving extra-long messages• Storage: Up to 500 messages can be saved in the internal memory of the B310As-938.• New message prompt
WLAN setup	<ul style="list-style-type: none">• 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
Firewall setup	<ul style="list-style-type: none">• Firewall Switch• LAN IP Filter• Virtual Server• DMZ Service
NAT setup	<ul style="list-style-type: none">• CONE NAT• Symmetric NAT• ALG
DHCP setup	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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

--	--	--



	 B310As-938TCPU -V100R001B326D1	

4 Web UI

4.1 Version Description

Web UI Version: 21.100.33.00.03

4.2 Web UI Specifications

Item	Specifications
1	Support recovery update

4.3 Known Limitations and Issues

Index	Case ID	Issue Description
1		

5 Software Vulnerabilities Fixes

[Software Vulnerabilities include Android Vulnerability, Third-party software Vulnerability, and Huawei Vulnerability]

[Android Vulnerability is from Google, which reported publicly.]

[Third-party software is a type of computer software that is sold together with or provided for free in Huawei products or solutions with the ownership of intellectual property rights (IPR) held by the original contributors. Third-party software can be but is not limited to: Purchased software, Software that is built in or attached to purchased hardware, Software in products of the original equipment manufacturer (OEM) or original design manufacturer (ODM), Software that is developed with technical contribution from partners (ownership of IPR all or partially held by the partners), Software that is legally obtained free of charge. The data of third-party software vulnerabilities fixes can be exported from PDM.]



If the table is excessively long, you can divide it into multiple ones by product version, or deliver it in an excel file with patch release notes and provide reference information in this section.]

[Huawei Vulnerability is Huawei own software' Vulnerability, which found by outside]

*Vulnerabilities information is available through CVE IDs in NVD (National Vulnerability Database) website:
<http://web.nvd.nist.gov/view/vuln/search>*

Remarks : Product inheritance Atpv2 platform Vulnerabilities

Software/Module name	Version	CVE ID	Vulnerability Description	Solution
linux_kernel	3.10	CVE-2016-8633	A buffer overflow vulnerability due to a lack of input filtering of incoming fragmented datagrams was found in the IP-over-1394 driver [firewire-net] in a fragment handling code in the Linux kernel. The vulnerability exists since firewire supported IPv4, i.e. since version 2.6.31 (year 2009) till version v4.9-rc4. A maliciously formed fragment with a respectively large datagram offset would cause a memcpy() past the datagram buffer, which would cause a system panic or possible arbitrary code execution. The flaw requires [firewire-net] module to be loaded and is remotely exploitable from connected firewire devices, but not over a local network.	Merge the patch: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=667121ace9dbafb368618dba_bcf07901c962ddac
linux_kernel	3.10	CVE-2016-2847	It is possible for a single process to cause an OOM condition by filling large pipes with data that are never read. A typical process filling 4096 pipes with 1 MB of data will use 4 GB of memory and there can be multiple such processes, up to a per-user-limit	Merge the patch: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=759c01142a5d0f364a462346168a56de28a80f52
linux_kernel	3.10	CVE-2016-3070	The trace_writeback_dirty_page implementation in include/trace/events/writeback.h in the Linux kernel before 4.4 improperly interacts with mm/migrate.c, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or	Merge the patch: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=42cb14b110a5698ccf26ce59c4441722605a3743



			<i>possibly have unspecified other impact by triggering a certain page move.</i>	
<i>linux kernel</i>	<i>3.10</i>	<i>CVE-2017-5967</i>	<i>The time subsystem in the Linux kernel, when CONFIG_TIMER_STATS is enabled, allows local users to discover real PID values (as distinguished from PID values inside a PID namespace) by reading the /proc/timer_list file, related to the print_timer function in kernel/time/timer_list.c and the __timer_stats_timer_set_start_info function in kernel/time/timer.c.</i>	<i>Merge the patch: https://git.kernel.org/pub/scm/linux/kernel/git/tip/tip.git/commit/?id=dfb4357da6ddbdf57d583ba64361c9d792b0e0b1</i>
<i>linux kernel</i>	<i>3.10</i>	<i>CVE-2017-5669</i>	<i>The do_shmat function in ipc/shm.c in the Linux kernel, through 4.9.12, does not restrict the address calculated by a certain rounding operation. This allows privileged local users to map page zero and, consequently, bypass a protection mechanism that exists for the mmap system call. This is possible by making crafted shmget and shmat system calls in a privileged context.</i>	<i>Merge the patch: https://github.com/torvalds/linux/commit/e1d35d4dc7f089e6c9c080d556feedf9c706f0c7</i>
<i>linux kernel</i>	<i>3.10</i>	<i>CVE-2017-5970</i>	<i>The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP options.</i>	<i>Merge the patch: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=34b2cef20f19c87999fff3da4071e66937db9644</i>
<i>linux kernel</i>	<i>3.10</i>	<i>CVE-2017-6214</i>	<i>The tcp_splice_read function in net/ipv4/tcp.c in the Linux kernel before 4.9.11 allows remote attackers to cause a denial of service (infinite loop and soft lockup) via vectors involving a TCP packet with the URG flag.</i>	<i>Merge the patch: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ccf7abb93af09ad0868ae9033d1ca8108bdaec82</i>
<i>linux_kernel</i>	<i>3.10, 3.18</i>	<i>CVE-2016-9794</i>	<i>Race condition in the snd_pcm_period_elapsed function in sound/core/pcm_lib.c in the ALSA subsystem in the Linux kernel before 4.7 allows local users to cause a denial of service (use-after-free) or</i>	<i>Merge the patch: https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=a27178e05b7c332522df40904f27674e36ee3757</i>



			<i>possibly have unspecified other impact via a crafted SNDRV_PCM_TRIGGER_S TART command.</i>	
<i>linux_kernel</i>	<i>3.10, 3.18</i>	<i>CVE-2015-9004</i>	<i>kernel/events/core.c in the Linux kernel before 3.19 mishandles counter grouping, which allows local users to gain privileges via a crafted application, related to the perf_pmu_register and perf_event_open functions.</i>	<i>Merge the patch: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c3c87e770458aa004bd7ed3f29945ff436fd6511</i>
<i>linux_kernel</i>	<i>3.10, 3.18</i>	<i>CVE-2017-0630</i>	<i>An information disclosure vulnerability in the kernel trace subsystem 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. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34277115.</i>	<i>Merge the patch: ANDROID-34277115</i>
<i>linux_kernel</i>	<i>3.10, 3.18</i>	<i>CVE-2017-7184</i>	<i>The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not validate certain size data after an XFRM_MSG_NEWAE update, which allows local users to obtain root privileges or cause a denial of service (heap-based out-of-bounds access) by leveraging the CAP_NET_ADMIN capability, as demonstrated during a Pwn2Own competition at CanSecWest 2017 for the Ubuntu 16.10 linux-image-* package 4.8.0.41.52.</i>	<i>Merge the patch: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f843ee6dd019bcece3e74e76ad9df0155655d0df</i>
<i>Android</i>	<i>4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2</i>	<i>CVE-2017-0598</i>	<i>An information disclosure vulnerability in the Framework APIs could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1,</i>	<i>Merge the patch: ./android-4.4.4_r2.0.1/platform/frameworks/base/0001-DO-NOT-MERGE-Check-bounds-in-offsetToPtr.bulletin.patch ./android-4.4.4_r2.0.1/platform/frameworks/base/0002-DO-NOT-MERGE-Throw-exception-if-slot-has-invalid-offset.bulletin.patch</i>



			6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-34128677.	
--	--	--	---	--