Product name	Confidentiality level
B525s-95a	CONFIDENTIAL
Product version	Total 9 pages
V1.0	

HUAWEI B525s-95a Release Notes

V1.0

Prepared by	B525s-95a Team	Date	2019-8-20
Reviewed by	B525s-95a Team	Date	2019-8-20
Approved by	B525s-95a Team	Date	2019-8-20

Huawei Technologies Co., Ltd.

Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2018-09-21	1.0	FW 81.190.01.03.00 WebUI 81.100.45.00.03	The 1th Version	Wwx479832
2018-10-20	2.0	FW 81.190.01.06.00 WebUI 81.100.45.01.03	The 2th Version	Wwx479832
2018-11-5	3.0	FW 81.190.01.08.00 WebUI 81.100.45.00.03	The 3th Version	Wwx479832
2018-11-26	4.0	FW 81.191.01.00.00 WebUI 81.100.29.00.03	The 4th Version	Wwx479832
2019-1-2	5.0	FW 81.191.03.00.00 WebUI 81.100.31.00.03	The 5th Version	Wwx479832
2019-1-21	6.0	FW 81.191.05.00.00 WebUI 81.100.31.01.03	The 6th Version	Wwx479832
2019-2-18	7.0	FW 81.191.07.00.00 WebUI 81.100.31.02.03	The 7th Version	Wwx479832
2019-2-27	8.0	FW 81.191.09.00.00 WebUI 81.100.31.02.03	The 8th Version	Wwx479832
2019-3-13	9.0	FW 81.191.11.00.00 WebUI 81.100.31.03.03	The 9th Version	Wwx479832
2019-8-20	10.0	FW 81.191.27.00.00 WebUI 81.100.33.03.03	The 10th Version	B525s-95a Team

Table of Contents

HUAWEI B525s-95a Release Notes V1.0

Abbreviations	description

1 Main Features

The B525s-95a mainly supports the following features:

- LTE data service up to 300 Mbit/s(cat 6)
- HSPA+ data service up to 21.6 Mbit/s
- HSDPA packet data service of up to 14.4 Mbit/s
- HSUPA data service up to 5.76 Mbit/s
- WCDMA PS domain data service of up to 384Kbps
- EDGE data service up to 236.8kbps
- GPRS data service up to 85.6 kbps
- CS voice service
- Data and SMS Service
- Support WiFi 2*2,2.4G; WiFi 3*3,5G ,WIFI 802.11a/b/g/n/ac，40MHz(11n)，80MHz (11ac) ，AP DBDC mode
- WEB UI, Auto connect
- Plug and play
- IPv6v4 dual stack
- Support Windows and MAC OS with the latest version..

2 Hardware

2.1 Version Description

Hardware Version:	WL1B520TM.Ver.A
Platform & Chipset:	Balong V722 WiFi 2.4G BCM43217 5G BCM4360

2.2 Hardware Specifications

Item	Specifications	
Technical standard	LTE	3GPP R10
	WCDMA	3GPP R8
	WLAN	IEEE 802.11a/b/g/n/ac
Operating	LTE	B1/3/8/38/40/41

Item	Specifications	
frequency	WCDMA	Band 1/8
	GSM	Band 2/3/5/8
	WLAN	2.4 GHz
	WLAN	5G
Internal memory	512 MB Flash,256 MB Memory	
Maximum transmitter power	UMTS: NA	
	WLAN	802.11b: 20 (+/-3) dBm
		802.11g: 17 (+/-3) dBm
		802.11n: 17 (+/-3) dBm
Receiver sensitivity	UMTS: NA	
	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	802.11a: Up to 54 Mbit/s	
	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)	
	802.11ac: HT80 MCS9 (1.3Gbit/s)	
Maximum power consumption	12 W	
Power supply	AC: 100–240 V	
	DC: 12 V, 2 A	
External interfaces	WAN/LAN: 4 RJ45,GE	
	SIM card interface: standard 6-pin SIM card interface	
Indicators	MODE	cyan: 4G mode blue: 3G mode yellow: 2G 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 five: Weak to Strong signal Off: out signal

Item	Specifications	
	WPS/WIFI	White Blink: WPS open On: WiFi is opened Off: WiFi is closed
	Power	On/Off
Button	Reset switch, WPS switch, Power switch	
Dimensions (D × W × H)	225 * 163 * 52/20 mm	
Weight	about 366.16 g (Does not contain the power adapter)	
Temperature	Operating: 0℃ to +40℃	
	Storage: -20℃ to +70℃	
Humidity	5% to 95% (non-condensing)	

2.3 Improvements in the Previous Version

Index	Case ID	Issue Description
NA		

2.4 Known Limitations and Issues

Index	Case ID	Issue Description
NA		

3 Firmware

3.1 Version Description xie

Firmware Version:	81.191.27.00.00
Baseline information	Balong V700R220C60B191
OS	Linux 3.10.100

3.2 Firmware Specifications

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 B525s-95a. • New message prompt

Item	Description
Network connection setup	• APN management: create, delete and edit. • Set up network connection
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
Firewall setup	• Firewall Switch • LAN IP Filter • Virtual Server • DMZ Service
NAT setup	• CONE NAT • Symmetric NAT • ALG • VPN passthrough
DHCP setup	• DHCP server enabling and disabling • Address pool of the DHCP server setup • DHCP lease time setup
IPv6v4 dual stack	DHCPv6/v4 server and client DNSv6/v4 server and client Display IPv6/v4 WAN address
Other	Network connection settings: • Automatic network selection and registration • Manual network selection and registration
	Network status display: signal, operator name, system mode, and so on.
	Selection of network connection types, for example: • Support LTE networks ON/OFF
	PIN management: activate/deactivate PIN, PIN lock, changing PIN, unblocking by using the PUK.

Item	Description
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
		See the DTS list

3.4 Known Limitations and Issues

Index	Case ID	Issue Description
1		

4 WebUI/HiLink

4.1 Version Description

WebUI/HiLink Version: 81.100.33.03.03

4.2 WebUI/HiLink Specifications

Item	Specifications

4.3 Improvement in the Previous Version

Index	Case ID	Issue Description
1	New Features	
2		
3		

4.4 Known Limitations and Issues

Index	Case ID	Issue Description
1	Unrealized Features	
2		
3		

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

Software/Module name	Version	CVE ID	Vulnerability Description	Solution
busybox	*1.9.1 1.21.*	*CVE-2017-16544*	*In the add_match function in libbb/lineedit.c in BusyBox through 1.27.2, the tab autocomplete feature of the shell, used to get a list of filenames in a directory, does not sanitize filenames and results in executing any escape sequence in the terminal. This could potentially result in code execution, arbitrary file writes, or other attacks.*	*https://git.busybox.net/busybox/commit/?id=c3797d40a1c57352192c6106cc0f435e7d9c11e8*
busybox	*1.9.1 1.21.*	*CVE-2017-15873*	*The get_next_block function in archival/libarchive/decompress_bunzip2.c in BusyBox 1.27.2 has an Integer Overflow that may lead to a write access violation.*	*https://git.busybox.net/busybox/commit/?id=0402cb32df015d9372578e3db27db47b33d5c7b0*
busybox	*1.9.1 1.21.*	*CVE-2011-5325*	*Directory traversal vulnerability in the BusyBox*	*https://git.busybox.net/busybox/commit/?id*

			implementation of tar before 1.22.0 v5 allows remote attackers to point to files outside the current working directory via a symlink	*=a116552869db5e7793ae10968eb3c962c69b3d8c*
linux_kernel	*3.10.100*	*CVE-2012-6703*	*Integer overflow in the snd_compr_allocate_buffer function in sound/core/compress_offload.c in the ALSA subsystem in the Linux kernel before 3.6-rc6-next-20120917 allows local users to cause a denial of service (insufficient memory allocation) or possibly have unspecified other impact via a crafted SNDRV_COMPRESS_SET_PARAMS ioctl call.*	CONFIRM:https://github.com/torvalds/linux/commit/b35cc8225845112a616e3a2266d2fde5ab13d3ab
linux_kernel	*3.10.100*	*CVE-2017-11176*	*The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact.*	CONFIRM:https://github.com/torvalds/linux/commit/f991af3daabaecff34684fd51fac80319d1baad1
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=667121ace9dbafb368618dbabcf07901c962ddac
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*	*Merge the patch:* https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=759c01

			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	142a5d0f364a462346168a56de28a80f52
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 possibly have unspecified other impact by triggering a certain page move.*	*Merge the patch:* https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=42cb14b110a5698ccf26ce59c4441722605a3743
linux kernel	*3.10*	*CVE-2017-5967*	*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.*	*Merge the patch:* https://git.kernel.org/pub/scm/linux/kernel/git/tip/tip.git/commit/?id=dfb4357da6ddbdf57d583ba64361c9d792b0e0b1
linux kernel	*3.10*	*CVE-2017-5669*	*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.*	*Merge the patch:* https://github.com/torvalds/linux/commit/e1d35d4dc7f089e6c9c080d556feedf9c706f0c7
linux kernel	*3.10*	*CVE-2017-5970*	*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.*	*Merge the patch: https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=34b2cef20f19c87999fff3da4071e66937db9644*

linux kernel	*3.10*	*CVE-2017-6214*	*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.*	*Merge the patch:* https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ccf7abb93af09ad0868ae9033d1ca8108bdaec82
linux_kernel	*3.10, 3.18*	*CVE-2016-9794*	*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 possibly have unspecified other impact via a crafted SNDRV_PCM_TRIGGER_START command.*	*Merge the patch:* https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=a27178e05b7c332522df40904f27674e36ee3757
linux_kernel	*3.10, 3.18*	*CVE-2015-9004*	*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.*	*Merge the patch:* https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c3c87e770458aa004bd7ed3f29945ff436fd6511
linux_kernel	*3.10, 3.18*	*CVE-2017-0630*	*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.*	*Merge the patch: ANDROID-34277115*
linux_kernel	*3.10, 3.18*	*CVE-2017-7184*	*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*	*Merge the patch:* https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=f843ee6dd019bcece3e74e76ad9df0155655d0df

			linux-image- package 4.8.0.41.52.*	
Android	*4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2*	*CVE-2017-0598*	*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, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-34128677.*	*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*
OpenSSL	*1.0.2k*	*NA*	*Update from 1.0.2j*	*Update OpenSSL from OpenSSL 1.0.2j to OpenSSL 1.0.2k*
linux_kernel	*3.10*	*CVE-2017-10661*	*The handling of the might_cancel queueing is not properly protected, so parallel operations on the file descriptor could race with each other and lead to list corruptions or use after free.*	*Merge the patch: A-36266767*
linux_kernel	*3.10*	*CVE-2017-0713*	*In the sfntly library used by libskia, a malformed font file could achieve privilege escalation due to an out-of-bounds read and probable write.*	*Merge the patch: A-32096780*

-