

Product name	Confidentiality level
E5885ls-93a	CONFIDENTIAL
Product version	Total 10 pages
V200R001	

E5885Ls-93aTCPU-V200R001B236D05SP01

C233 Firmware Release Notes

V2.0

Prepared by	E5885ls-93a Team	Date	2017-7-18
Reviewed by	E5885ls-93a Team	Date	2017-7-18
Approved by	E5885ls-93a Team	Date	2017-7-18



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2017-7-18	2.0	FW 21.236.05.01.233	The 2nd Version	E5885ls-93a 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	5
2.4	Known Limitations and Issues	5
3	Firmware	5
3.1	Version Description	5
3.2	Firmware Specifications	5
3.3	Improvement in the Previous Version	6
3.4	Known Limitations and Issues	6
4	Software Vulnerabilities Fixes.....	6



1 Main Features

The E5885Ls-93a supports the following standards:

- 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 296kbps
- GPRS data service up to 85.6 kbps
- Data and SMS Service
- Support WiFi 2*2; 2.4G/5G ,WIFI 802.11a/b/g/n/ac, 40MHz(11n), 80MHz (11ac)
- Micro USB 2.0 interface
- WEB UI, Auto connect
- Plug and play
- Standard USB2.0
- Support Windows and MAC OS with the latest version..

2 Hardware

2.1 Version Description

Hardware Version: CL1E5885SM
Platform & Chipset: Balong V722
WiFi Hisi 1151

2.2 Hardware Specifications

Item	Specifications	
Technical Standard	LTE	3GPP R10
	WCDMA	3GPP R8
Operating Frequency	LTE	LTE FDD: B1/B2/B3/B4/B5/B7/B8/B20/B19 LTE TDD: B38/B40/B41
	WCDMA	B1/B2/B4/B5/B6/B8/B19
	GSM	850/900/1800/1900Mhz
Memory	256MB	
WLAN Rate	802.11b: Up to 11 Mbit/s	
	802.11g: Up to 54 Mbit/s	



	802.11n: HT20: Support MCS0–MCS7; Up to 72.2 Mbit/s. Support MCS8–MCS15; Up to 144.4 Mbit/s. HT40: Support MCS0–MCS7; Up to 150 Mbit/s. Support MCS8–MCS15; Up to 340 Mbit/s.
External Interfaces	USB: Micro USB 2.0
	LCD
	Ethernet port: RJ45
	Standard microSD card interface
	SIM/USIM card: USIM
Keys	1 Power,1 Reset,1 WPS
Battery	6400mAH
Ambient Temperature	Operating: 0°C to +35°C Storage: -20°C to +60°C
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

Firmware Version:	21.236.05.01.233
Baseline information	Balong V7R22 C30B236
OS	Linux 3.10.59

3.2 Firmware Specifications

Item	Specifications



3.3 Improvement in the Previous Version

Index	Case ID	Issue Description
1	CA配置	当注册上 CA 网络,需要显示为 4G+ （配置 CA）
2	中文SSID	用户修改SSID时，能够支持中文SSID.

3.4 Known Limitations and Issues

Index	Case ID	Issue Description
1		

4 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
----------------------	---------	--------	---------------------------	----------



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.	https://github.com/torvalds/linux/commit/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 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	https://github.com/torvalds/linux/commit/759c01142a5d0f364a462346168a56de28a80f52
linux_kernel	3.10	CVE-2016-3070	A security flaw was found in the Linux kernel that an attempt to move page mapped by AIO ring buffer to the other node triggers NULL pointer dereference at trace_writeback_dirty_page(), because aio_fs_backing_dev_info.dev is 0.	https://github.com/torvalds/linux/commit/42cb14b110a5698ccf26ce59c4441722605a3743#diff-8e2530775024feb6361f8a93e833d3c1
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	http://git.kernel.org/cgit/linux/kernel/git/tip/tip.git/commit/?id=dfb4357da6ddbdf57d583ba64361c9d792b0e0b1



			kernel/time/timer.c.	
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.	https://github.com/torvalds/linux/commit/e1d35d4dc7f089e6c9c080d556feedf9c706f0c7
linux kernel	3.10	CVE-2017-5970	A vulnerability was found in the Linux kernel where having malicious IP options present would cause the ipv4_pktinfo_prepare() function to drop/free the dst. This could result in a system crash or possible privilege escalation	https://github.com/torvalds/linux/commit/34b2cef20f19c87999fff3da4071e66937db9644
linux kernel	3.10	CVE-2017-6214	A flaw was found in the Linux kernel's handling of packets with the URG flag. Applications using the splice() and tcp_splice_read() functionality can allow a remote attacker to force the kernel to enter a condition in which it can loop indefinitely	https://github.com/torvalds/linux/commit/ccf7abb93af09ad0868ae9033d1ca8108bdaecc82
linux_kernel	3.10, 3.18	CVE-2016-9794	A 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. The fix is designed to move the kill_fasync function call inside the stream lock.	https://github.com/torvalds/linux/commit/3aa02cb664c5fb1042958c8d1aa8c35055a2ebc4
linux_kernel	3.10, 3.18	CVE-2015-9004	llowing perf event groups to span multiple CPUs or different task contexts could allow perf to reduce the event reference count to zero leading to a NULL pointer dereference, potentially causing elevation of	https://github.com/torvalds/linux/commit/c3c87e770458aa004bd7ed3f29945ff436fd6511



			privilege. The fix is designed to restrict perf event groups to the same context in such a way that all the events in a group are for the same CPU or the same process.	
linux_kernel	3.10, 3.18	CVE-2017-0630	Information disclosure in the kernel could reveal the locations of strings that are used in some printk messages that describe the layout of the constants section of the kernel, which could potentially be used to weaken KASLR. The fix is designed to mask all address to 0x0 but preserve the message format.	Merge the pathes
linux_kernel	3.10, 3.18	CVE-2017-7184	When a new xfrm state is created during an XFRM_MSG_NEWSA call we validate the user supplied replay_esn to ensure that the size is valid and to ensure that the replay_window size is within the allocated buffer. However later it is possible to update this replay_esn via a XFRM_MSG_NEWAE call. There we again validate the size of the supplied buffer matches the existing state and if so inject the contents. We do not at this point check that the replay_window is within the allocated memory. This leads to out-of-bounds reads and writes triggered by netlink packets. This leads to memory corruption and the potential for privilege escalation. The fix is designed to add additional validation of the replay_window to prevent the potential memory corruption.	https://github.com/torvalds/linux/commit/677e806da4d916052585301785d847c3b3e6186a
linux_kernel	3.10	CVE-2014-9940	The regulator_ena_gpio_free function in drivers/regulator/core.c in the Linux kernel before 3.19 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted application.	https://github.com/torvalds/linux/commit/60a2362f769cf549dc466134efe71c8bf9fbaba
Android	4.4.4, 5.0.2, 5.1.1, 6.0,	CVE-2017-0598	The native CursorWindow class, which is used for	Merge the pathes



	6.0.1, 7.0, 7.1.1, 7.1.2		adapting the ContentProvide.query() result from ashmem, does not check if the values for the offset and size of the field belong to the region of the mapped ashmem area. This could enable the querying application to read values from a different memory location than the data provided by ContentProvider. The fix is designed to verify the size of the ashmem region and to add a default argument bufferSize to check the offset.	
linux_kernel	3.10	CVE-2015-1465, CVE-2015-5364, CVE-2016-9555, CVE-2016-7916	A vulnerability was found in the Linux kernel	Merge the pathes
linux_kernel	3.10	CVE-2017-9074, CVE-2017-7487, CVE-2017-9242	A vulnerability was found in the Linux kernel	Merge the pathes
linux_kernel	3.10	CVE-2017-8890, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077	A vulnerability was found in the Linux kernel	Merge the pathes