

E5885Ls-93aTCPU-V200R001B190D61SP00C1505

Release Notes

Prepared by	E5885Ls-93a Team	Date	2018/12/05
Reviewed by	E5885Ls-93a Team	Date	2018/12/05
Approved by	E5885Ls-93a Team	Date	2018/12/05



Huawei Technologies Co., Ltd.

All rights reserved

Table of Contents

1.	Main Features	3
2.	Hardware	3
	2.1Version Description	3
	2.2Hardware Specifications	4
3.	Firmware.....	4
	3.1Version Description	4
	3.2Improvement in the Previous Version.....	5
	3.3Known 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 Ver. A
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)	

3. Firmware

3.1 Version Description

Firmware Version:	21.190.61.00.1505
WEBUI Version:	21.100.46.00.1505
Baseline information	Balong V7R22 C60B189

3.2 Improvement in the Previous Version

Index	Description
1	1.SIM LOCK 2.SSID 3.WIFI KEY 4.Login IP 5.Login Account 6.Web Language 7.Help Language 8.APN Autoadapter 9.APN Retry 10.Operator Name 11.Roaming white list 12.SMS 13.My number 14.Change string 15.Dual IMSI 16.multi-IMSI 17.Steering of Roaming 18.EPLMN 19.EFSPDI 20.IMEI SVN 21.Network search mode 22.Partner Operator 23.Roaming 24.Add parameters 25.Data Roaming 26.Auto Disconnect Interval 27.Auto-select network 28.Device Information 29.Multiple IMSI

3.3 Known Limitations and Issues

Index	Issue Description
NA	

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	Impact Description
linux_kernel	3.10.100	CVE-2017-10661	Race condition in fs/timerfd.c in the Linux kernel before 4.10.15 allows local users to gain privileges or cause a denial of service (list corruption or use-after-free) via simultaneous file-descriptor operations that leverage improper might_cancel queueing.	https://github.com/torvalds/linux/commit/1e38da300e1e395a15048b0af1e5305bd91402f6
linux_kernel	3.10.100	CVE-2017-14106	The tcp_disconnect function in net/ipv4/tcp.c in the Linux kernel before 4.12 allows local users to cause a denial of service	https://github.com/torvalds/linux/commit/499350a5a6e7512d9ed369ed63a4244b6536f4f8

			(<i>__tcp_select_w indow divide-by- zero error and system crash</i>) by triggering a disconnect within a certain <i>tcp_recvmg code path.</i>	
<i>linux_kern el</i>	<i>3.10, 3.18</i>	<i>CVE- 2017-0630</i>	<i>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.</i>	<i>Merge the pathes</i>
<i>linux_kern el</i>	<i>3.10, 3.18</i>	<i>CVE- 2017-7184</i>	<i>When a new xfrm state is created during an XFRM_MSG_N EWSA 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_N EWAE call. There we again validate the size of the supplied buffer matches the existing state and if so</i>	<i>https://github.com/torvalds/linux/commit/677e806da4d916052585301785d847c3b3e6186a</i>

			<p><i>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.</i></p>	
linux_kernel	3.10	CVE-2014-9940	<p><i>The regulator_enable_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.</i></p>	<p>https://github.com/torvalds/linux/commit/60a2362f769cf549dc466134efe71c8bf9fbaaba</p>
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	<p><i>The native CursorWindow class, which is used for adapting the ContentProvider.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</i></p>	<p><i>Merge the pathes</i></p>

			<i>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.</i>	
--	--	--	---	--