

Product name	Confidentiality level
E5770s-923	CONFIDENTIAL
Product version	Total 9 pages
V1.0	

HUAWEI E5770s-923 Release Notes V1.0

Prepared by	E5770s-923 Team	Date	2017/04/17
-------------	-----------------	------	------------



Huawei Technologies Co., Ltd.



Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2017/04/17	1.0	FW 21.326.01.00.00	The first Version	E5770s-923 Team
2018/01/18	1.0	FW 21.329.01.00.00	MR Version	E5770s-923 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	6
3.1	Version Description	6
3.2	Firmware Specifications	6
3.3	Improvement in the Previous Version	6
3.4	Known Limitations and Issues	6
4	WebUI/HiLink	6
4.1	Version Description	6
4.2	WebUI/HiLink Specifications	7
4.3	Improvement in the Previous Version	7
4.4	Known Limitations and Issues	7
5	Software Vulnerabilities Fixes	7
6	Accessory Product from other Vendor	13
6.1	Version Description	13
6.2	Known Limitations and Issues	14
7	Others	14
8	Reference	14



HUAWEI E5770s-923 Release Notes V1.0

Abbreviations	Description

1 Main Features

The E5770s-923 supports the following features:

- *LTE cat4 data service up to 150Mbit/s (Downlink) and 50Mbit/s(Uplink)*
- *DC-HSPA+ data service up to 43.2 Mbit/s*
- *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 384 Kbit/s*
- *Equalizer and receive diversity*
- *Data and SMS Service*
- *WEB UI, Auto connect*
- *Plug and play*
- *Standard USB2.0*
- *Support WiFi 2.4GHz*

2 Hardware

2.1 Version Description

Hardware Version:	CL1E5770SM01 Ver.A
Platform & Chipset:	Balong Hi6921 V7R11M, RTL8192

2.2 Hardware Specifications

Item	Specifications	
Technical Standard	3GPP	R99/R5/R6/R7/R8/R9
	IEEE	802.11b/g/n
Operating Frequency	LTE	FDD B1(2100 MHz)/B3(1800 MHz)/B7(2600 MHz) TDD B38(2600 MHz)/B40(2400 MHz)/B41(2600 MHz)
	UMTS	DC-HSPA+/HSPA+/HSPA/UMTS: B1(2100 MHz)/B8(900 MHz) B2(1900MHz)/B3(1800MHz)/B8(900MHz)/B5(850MHz)
Maximum Transmitter Power	LTE	+23dBm (Class 3)
	UMTS	+24dBm (Class 3)



Maximum Power Consumption	4W
Memory	128M NAND Flash, 128M DDR
WLAN Rate	802.11b: 11Mbit/s, 5.5Mbit/s, 2Mbit/s, 1Mbit/s 802.11g: 54Mbit/s, 48Mbit/s, 36Mbit/s, 24Mbit/s, 18Mbit/s, 12Mbit/s, 9Mbit/s, 6Mbit/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 300 Mbit/s
External Interfaces	USB: Standard USB2.0
	Ethernet port: RJ45
	Micro USB interface
	LCD
	SIM/USIM card: 6pin, 1.8/3V
	Standard microSD card interface
Display	LCD
Keys	Power switch, WPS switch, Reset switch
Antenna	Internal
Static Receiver Sensitivity	Compliant with 3GPP TS 36.101(R9) for LTE, TS 25.101(R8) for UMTS.
Battery	5200mAh
Dimensions (D × W × H)	106.0 mm × 68.4 mm × 22.5 mm
Weight	about 200 g (including the battery)
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
Hardware Version		CL1E5770SM01 Ver.A
Previous Hardware Version		NA
NA		

2.4 Known Limitations and Issues

Index	Case ID	Issue Description
NA		NA



3 Firmware

3.1 Version Description

Firmware Version: 21.329.01.00.00
Baseline information Hi6921 V7R11M

3.2 Firmware Specifications

Item	Specifications

3.3 Improvement in the Previous Version

Index	Case ID	Issue Description
Firmware Version		21.329.01.00.00
Previous Firmware Version		21.326.01.00.00
1	NA	
2	NA	
3	NA	
4	NA	
5	NA	
6	NA	
7	NA	

3.4 Known Limitations and Issues

Index	Case ID	Issue Description
1	Unrealized Features	NA
2		
3		

4 WebUI/HiLink

4.1 Version Description

WebUI/HiLink Version: 17.100.19.01.00



4.2 WebUI/HiLink Specifications

Item	Specifications
NA	

4.3 Improvement in the Previous Version

Index	Case ID	Issue Description
WebUI Version		17.100.19.01.00
Previous Version	WebUI	N/A
1		
2		
3		

4.4 Known Limitations and Issues

Index	Case ID	Issue Description
1	NA	
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
linux_kernel	3.10, 3.18	CVE-2016-10229	A leftover buffer pointer on the kernel stack, in conjunction with insufficient checks on the state of data, could be used by a remote attacker to generate a heap buffer overflow in the kernel, potentially leading to remote code execution. The fix is designed to eliminate the possibility of overflow by making the checksum implementation more robust.	Google 2017 4# https://github.com/torvalds/linux/commit/197c949e7798fbf28cfadc69d9ca0c2abbf93191
linux_kernel	3.10, 3.18	CVE-2017-0571	Memory corruption in the _dhd_wlfc_reorderinfo_indicate function due to a missing length validation could potentially lead to elevation of privilege. The fix is designed to prevent the kernel heap corruption condition by adding appropriate buffer length validation.	Google 2017 4# http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0571
linux_kernel	3.1	CVE-2014-2706	A race condition in the mac80211 subsystem, in the Linux kernel before 3.13.7, allows remote attackers to cause a denial of service (system crash) via network traffic that improperly interacts with the WLAN_STA_PS_STA state (aka power-save mode), related to sta_info.c and tx.c. The fix is designed to synchronize the paths with a new lock.	Google 2017 4# https://github.com/torvalds/linux/commit/1d147bfa64293b2723c4fec50922168658e613ba
linux_kernel	3.10, 3.18	CVE-2016-7097	The filesystem implementation in the Linux kernel through 4.8.2 preserves the setgid bit during a setxattr call, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions. The fix is designed clear the setgid bit.	Google 2017 4# https://github.com/torvalds/linux/commit/073931017b49d9458aa351605b43a7e34598caef



linux_kernel	3.4.5	CVE-2012-2663	extensions/libxt_tcp.c in iptables through 1.4.21 does not match TCP SYN+FIN packets in --syn rules, which might allow remote attackers to bypass intended firewall restrictions via crafted packets. NOTE: the CVE-2012-6638 fix makes this issue less relevant.	http://www.spinics.net/lists/netfilter-devel/msg21248.html
linux_kernel	3.4.5	CVE-2017-0710	Technical details: A process with CAP_SYS_RESOURCE bypasses the permission check allowing arbitrary ptrace access. Fix details: The fix replaced CAP_SYS_RESOURCE with CAP_SYS_PTRACE for processes needing ptrace capability, and removed the CAP_SYS_RESOURCE bypass.	Google 2017 7# https://source.android.com/security/bulletin/2017-07-01
linux_kernel	3.4.5	CVE-2016-9555	The sctp_sf_ootb function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk, which allows remote attackers to cause a denial of service (out-of-bounds slab access) or possibly have unspecified other impact via crafted SCTP data.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=bf911e985d6bbaa328c20c3e05f4eb03de11fdd6
linux_kernel	3.4.5	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.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=2423496af35d94a87156b063ea5cedffc10a70a1



linux_kernel	3.4.5	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.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=ee0d8d8482345ff97a75a7d747efc309f13b0d80
linux_kernel	3.4.5	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.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=232cd35d0804cc241eb887bb8d4d9b3b9881c64a
linux_kernel	3.4.5	CVE-2017-8890	The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=657831ffc38e30092a2d5f03d385d710eb88b09a
linux_kernel	3.4.5	CVE-2017-9075	The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=fdcee2cbb8438702ea1b328fb6e0ac5e9a40c7f8



linux_kernel	3.4.5	CVE-2017-9076	The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=83eaddab4378db256d00d295bda6ca997cd13a52
linux_kernel	3.4.5	CVE-2017-9077	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=83eaddab4378db256d00d295bda6ca997cd13a52
linux_kernel	3.4.5	CVE-2016-4913	The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing \0 characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=99d825822eade8d827a1817357c6bf3f889a552d6
linux_kernel	3.4.5	CVE-2017-7472	The KEYS subsystem in the Linux kernel before 4.10.13 allows local users to cause a denial of service (memory consumption) via a series of KEY_REQKEY_DEFL_TH_READ_KEYRING keyctl_set_reqkey_keyring calls.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c9f838d104fed6f2f61d68164712e3204bf5271b



linux_kernel	3.4.5	CVE-2015-8966	arch/arm/kernel/sys_oabi-compat.c in the Linux kernel before 4.4 allows local users to gain privileges via a crafted (1) F_OFD_GETLK, (2) F_OFD_SETLK, or (3) F_OFD_SETLKW command in an fcntl64 system call.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=76cc404bfdc0d419c720de4daaf2584542734f42
linux_kernel	3.4.5	CVE-2016-7117	Use-after-free vulnerability in the __sys_recvmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmsg system call that is mishandled during error processing.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=34b88a68f26a75e4fde4796f1a49c40f82234b7d
linux_kernel	3.4.5	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.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c27927e372f0785f3303e8fad94b85945e2c97b7



linux_kernel	3.4.5	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 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.	https://github.com/torvalds/linux/commit/5649645d725c73df4302428ee4e02c869248b4c5
linux_kernel	3.4.5	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.	https://github.com/torvalds/linux/commit/37863c43b2c6464f252862bf2e9768264e961678
linux_kernel	3.4.5	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.	https://github.com/torvalds/linux/commit/1c0edc3633b56000e18d82fc241e3995ca18a69e
linux_kernel	3.4.5	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_AS SOCIATION descriptor.	https://github.com/torvalds/linux/commit/bd7a3fe770ebd8391d1c7d072ff88e9e76d063eb

6 Accessory Product from other Vendor

6.1 Version Description

Accessory Product Version:



6.2 Known Limitations and Issues

7 Others

8 Reference