E5577Cs-321TCPU-V200R001B333D63SP00C1217

Release Notes

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by | E5577Cs-321 Team | Date | 20181213 |
| Reviewed by | E5577Cs-321 Team | Date | 20181213 |
| Approved by | E5577Cs-321 Team | Date | 20181213 |



Huawei Technologies Co., Ltd.

All rights reserved

Table of Contents

[1. Main Features 3](#_Toc524110263)

[2. Hardware 3](#_Toc524110264)

[**2.1** **Version Description** 3](#_Toc524110265)

[**2.2** **Hardware Specifications** 4](#_Toc524110266)

[3. Firmware 4](#_Toc524110267)

[**3.1** **Version Description** 4](#_Toc524110268)

[**3.2** **Improvement in the Previous Version** 5](#_Toc524110269)

[**3.3** **Known Limitations and Issues** 5](#_Toc524110270)

[4. Software Vulnerabilities Fixes 5](#_Toc524110271)

# Main Features

The E5577Cs-321 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/5GHz

# Hardware

## **Version Description**

|  |  |
| --- | --- |
| Hardware Version: | CL1E5573SM11 |
| Platform & Chipset: | Balong Hi6921 V7R11M, Broadcomm 43241 |

## **Hardware Specifications**

| Item | Specifications | |
| --- | --- | --- |
| Technical Standard | 3GPP | R99/R5/R6/R7/R8/R9 |
| IEEE | 802.11a/b/g/n |
| Operating Frequency | LTE | FDD B1/B3/B5/B7/B8/B20 |
| UMTS | B1,B2,B5,B8 |
| Maximum Transmitter Power | LTE | +23dBm (Class 3) |
| UMTS | +24dBm (Class 3) |
| Maximum Power Consumption | 3.5W | |
| 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  802.11a: 54Mbit/s, 48Mbit/s, 36Mbit/s, 24Mbit/s, 18Mbit/s, 12Mbit/s, 9Mbit/s, 6Mbit/s  802.11n: MCS0-MCS7(WiFi 1x1), MSC0-MCS15(WiFi 2x2) | |
| External Interfaces | USB: Standard USB2.0 | |
| LCD | |
| SIM/USIM card: 6pin, 1.8/3V | |
| Standard microSD card interface | |
| Display | LCD | |
| Keys | 1 Power, 1 Reset，1 Menu | |
| Antenna | Internal | |
| Static Receiver Sensitivity | Compliant with 3GPP TS 36.101(R9) for LTE, TS 25.101(R8) for UMTS. | |
|  | |
| Battery | 1500mAh | |
| Dimensions (D × W × H) | **96.8mm\*58mm\*13.5mm** | |
| Weight | <120g(include Battery) | |
| Ambient Temperature | 0-35°C | |
| Humidity | 5%-95% | |

# Firmware

## **Version Description**

|  |  |
| --- | --- |
| Firmware Version:  WEBUI Version: | 21.333.63.00.1217  17.100.20.06.1217 |
| Baseline information | Hi6921 V7R11M |
|  |  |

## **Improvement in the Previous Version**

| Index | Description |
| --- | --- |
| 1 | 1、Update APN List,Operator Name,Partner Operator,Language sheet. 2、Add Signal parameter Display in deviceinformation page |

## **Known Limitations and Issues**

| Index | Issue Description |
| --- | --- |
| NA |  |

# 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*](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 ipxitf\_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=99d825822eade8d827a1817357cbf3f889a552d6 |
| 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\_THREAD\_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](https://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\_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing. | http:[//git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=34b88a68f26a75e4fded796f1a49c40f82234b7d](http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=34b88a68f26a75e4fded796f1a49c40f82234b7d) |
| busybox | 1.21.1 | 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 | 1.21.1 | CVE-2016-6301 | The recv\_and\_process\_client\_pkt function in networking/ntpd.c in busybox allows remote attackers to cause a denial of service (CPU and bandwidth consumption) via a forged NTP packet, which triggers a communication loop. | https://git.busybox.net/busybox/commit/?id=150dc7a2b483b8338a3e185c478b4b23ee884e71 |
| linux\_kernel | 3.6.5 | 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 | 3.6.5 | 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\_ASSOCIATION descriptor. | https://github.com/torvalds/linux/commit/bd7a3fe770ebd8391d1c7d072ff88e9e76d063eb |
| linux\_kernel | 3.6.5 | 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 | 3.6.5 | CVE-2017-0427 | An elevation of privilege vulnerability in the kernel file system could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31495866. |  |