|  |  |
| --- | --- |
| Product name | Confidentiality level |
| B612s | CONFIDENTIAL |
| Product version | Total 10pages |
| V1.0 |

B612s-52dTCPU-V100R001B196D03SP00C00

Firmware Release Notes

V1.0

|  |  |  |  |
| --- | --- | --- | --- |
| Prepared by | B612s Team | Date | 2018-4-16 |
| Reviewed by | B612s Team | Date | 2018-4-16 |
| Approved by | B612s Team | Date | 2018-4-16 |



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Revision version | FW-WebUI/HiLink  Version | Change Description | Author |
| 2018.4.28 | 1.0 | 11.195.01.06.00 | The 1st Version | Weibangjin wwx479832 |
| 2018.5.24 | 2.0 | 11.196.01.00.00 | The 2st Version | Weibangjin wwx479832 |
| 2018.6.5 | 3.0 | 11.196.03.00.00 | The 3st Version | Weibangjin wwx479832 |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[1 Main Features 4](#_Toc477513365)

[2 Hardware 4](#_Toc477513366)

[**2.1** **Version Description** 4](#_Toc477513367)

[**2.2** **Hardware Specifications** 4](#_Toc477513368)

[**2.3** **Improvements in the Previous Version** 6](#_Toc477513369)

[**2.4** **Known Limitations and Issues** 6](#_Toc477513370)

[3 Firmware 6](#_Toc477513371)

[**3.1** **Version Description** 6](#_Toc477513372)

[**3.2** **Firmware Specifications** 6](#_Toc477513373)

[**3.3** **Improvement in the Previous Version** 7](#_Toc477513374)

[**3.4** **Known Limitations and Issues** 7](#_Toc477513375)

[4 WebUI/HiLink 8](#_Toc477513376)

[**4.1** **Version Description** 8](#_Toc477513377)

[**4.2** **WebUI/HiLink Specifications** 8](#_Toc477513378)

[**4.3** **Improvement in the Previous Version** 8](#_Toc477513379)

[**4.4** **Known Limitations and Issues** 8](#_Toc477513380)

[5 Software Vulnerabilities Fixes 8](#_Toc477513381)

B612s Firmware Release Notes V1.0

|  |  |
| --- | --- |
| Abbreviations | description |
|  |  |
|  |  |

# Main Features

The B612s mainly supports the following features:

* LTE Cat6 4\*4 MIMO，FDD 300/50Mbps@20MHz，TDD 220/10Mbps@20MHz
* DC HSPA: 42 Mbps(downlink)/5.76 Mbps(Uplink)
* HSPA: 14.4 Mbps(downlink)/5.76 Mbps(Uplink)
* EDGE：296 Kbps (downlink)/236.8 Kbps(Uplink)
* CS voice service
* Data and SMS Service
* Support WiFi 2\*2 2.4G; WIFI 802.11 /b/g/n,40MHz(11n)
* 4GE 1POTS
* WEB UI, Auto connect
* LED indicators

Windows XP SP3, Windows Vista SP1/SP2, Windows 7, Windows 8, Windows 8.1 (does not support Windows RT), MAC OS X 10.7, 10.8 and 10.9 with latest upgrades

# Hardware

## **Version Description**

|  |  |
| --- | --- |
| Hardware Version: | **WL1B612M04 Ver.A** |
| Platform & Chipset: | Balong Hi6950 |

## **Hardware Specifications**

| Item | | Specifications | | | |
| --- | --- | --- | --- | --- | --- |
| Technical standard | | WAN: LTE | | | |
| WLAN: IEEE 802.11b/g/n/ac | | | |
| Operating frequency | B612s-52d | LTE: Band2, Band4, Band5,Band7, Band28, Band41, Band42, Band43,Band40(B40:2300~2390MHz,B41:2545~2655MHz) | | | |
| UMTS: Band2,Band4 Band5 | | | |
| GSM : Band2, Band3, Band5, Band8 | | | |
| WiFi: 2.4G | | | |
|  | | | |
|  | | | |
| Maximum transmitter power | | UMTS: NA | | | |
| WLAN | | 802.11b: 16 (+/-3) dBm | |
| 802.11g: 17 (+/-3) dBm | |
| 802.11n: 17 (+/-3) dBm | |
| Receiver sensitivity | | UMTS: NA | | | |
| WLAN 802.11b | | | -83 dBm@11 Mbit/s |
| -89 dBm@1 Mbit/s |
| WLAN 802.11g: -69 dBm@54 Mbit/s | | | |
| WLAN 802.11n: -67 dBm@65 Mbit/s | | | |
| WLAN speed | | 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) | | | |
| Maximum power consumption | | 12 W | | | |
| Power supply | | AC: 100–240 V | | | |
| DC: 12 V, 1 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: Ethernet 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 three: Weak to Strong signal  Off: out signal | | |
| WPS/WIFI | White Blink: WPS open  On: WiFi is opened  Off: WiFi is closed | | |
| LAN | White Blink: Data transfer  Off: No connect ether cable  On: connect ether cable | | |
| Power | On/Off | | |
| Button | | Reset switch, WPS switch, Power switch | | | |
| Dimensions (D × W × H) | | 240mm\*155mm\*78mm | | | |
| Weight | | about 600g (Does not contain the power adapter) | | | |
| Temperature | | Operating: 0℃ to +40℃ | | | |
| Storage: -20℃ to +70℃ | | | |
| Humidity | | 5% to 95% ( non-condensing) | | | |

## **Improvements in the Previous Version**

| Index | Case ID | Issue Description |
| --- | --- | --- |
| NA |  |  |

## **Known Limitations and Issues**

| Index | Case ID | Issue Description |
| --- | --- | --- |
| NA |  |  |

# Firmware

## **Version Description**

|  |  |
| --- | --- |
| Firmware Version: | 11.196.03.00.00 |
| Baseline information | BalongV700R500C31B196 |
| OS | RTos / linux 3.10 |
|  |  |

## **Firmware Specifications**

| 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 pass-through |
| DHCP setup | * DHCP server enabling and disabling * Address pool of the DHCP server setup * DHCP lease time setup |
| Other | * Automatic network selection and registration * Manual network selection and registration |
| Network status display: signal, operator name, system mode, and so on. |

## **Improvement in the Previous Version**

| Index | Case ID | Issue Description |
| --- | --- | --- |
|  |  |  |
|  |  |  |

## **Known Limitations and Issues**

|  |  |  |
| --- | --- | --- |
| **Index** | **Case ID** | **Issue Description** |
|  |  |  |

# WebUI/HiLink

## **Version Description**

WebUI/HiLink Version: **21.100.44.00.03**

## **WebUI/HiLink Specifications**

|  |  |
| --- | --- |
| Item | Specifications |
|  |  |
|  |  |

## **Improvement in the Previous Version**

|  |  |  |
| --- | --- | --- |
| **Index** | **Case ID** | **Issue Description** |
|  |  |  |
|  |  |  |
|  |  |  |

## **Known Limitations and Issues**

|  |  |  |
| --- | --- | --- |
| **Index** | **Case ID** | **Issue Description** |
|  |  |  |
|  |  |  |
|  |  |  |

# 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** |
| kernel | 4.10 | 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. | Merge in package |
| kernel | 4.10 | 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. | Merge in package |
| kernel | 4.10 | 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 (\_\_tcp\_select\_window divide-by-zero error and system crash) by triggering a disconnect within a certain tcp\_recvmsg code path. | Merge in package |
| kernel | 4.10 | CVE-2016-4805 | Use-after-free vulnerability in drivers/net/ppp/ppp\_generic.c in the Linux kernel before 4.5.2 allows local users to cause a denial of service (memory corruption and system crash, or spinlock) or possibly have unspecified other impact by removing a network namespace, related to the ppp\_register\_net\_channel and ppp\_unregister\_channel functions. | Merge in package |
| kernel | 4.10 | CVE-2017-7542 | The ip6\_find\_1stfragopt function in net/ipv6/output\_core.c in the Linux kernel through 4.12.3 allows local users to cause a denial of service (integer overflow and infinite loop) by leveraging the ability to open a raw socket. | Merge in package |
| kernel | 4.10 | CVE-2017-5972 | The TCP stack in the Linux kernel 3.x does not properly implement a SYN cookie protection mechanism for the case of a fast network connection, which allows remote attackers to cause a denial of service (CPU consumption) by sending many TCP SYN packets, as demonstrated by an attack against the kernel-3.10.0 package in CentOS Linux 7. NOTE: third parties have been unable to discern any relationship between the GitHub Engineering finding and the Trigemini.c attack code. | Merge in package |
|  | 4.10 | 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. | Merge in package |
| kernel | 4.10 | CVE-2017-2671 | The ping\_unhash function in net/ipv4/ping.c in the Linux kernel through 4.10.8 is too late in obtaining a certain lock and consequently cannot ensure that disconnect function calls are safe, which allows local users to cause a denial of service (panic) by leveraging access to the protocol value of IPPROTO\_ICMP in a socket system call. | Merge in package |
|  | 4.10 | CVE-2015-1465 | The IPv4 implementation in the Linux kernel before 3.18.8 does not properly consider the length of the Read-Copy Update (RCU) grace period for redirecting lookups in the absence of caching, which allows remote attackers to cause a denial of service (memory consumption or system crash) via a flood of packets. | Merge in package |
| kernel | 4.10 | CVE-2015-5364 | The (1) udp\_recvmsg and (2) udpv6\_recvmsg functions in the Linux kernel before 4.0.6 provide inappropriate -EAGAIN return values, which allows remote attackers to cause a denial of service (EPOLLET epoll application read outage) via an incorrect checksum in a UDP packet, | Merge in package |
| kernel | 4.10 | 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. | Merge in package |
| kernel |  | CVE-2016-7916 | Race condition in the environ\_read function in fs/proc/base.c in the Linux kernel before 4.5.4 allows local users to obtain sensitive information from kernel memory by reading a /proc/\*/environ file during a process-setup time interval in which environment-variable copying is incomplete. | Merge in package |
| ffmpeg | 2.8.9 | CVE-2017-7863 CVE-2017-7866 | FFmpeg before 2017-02-04 has an out-of-bounds write caused by a heap-based buffer overflow related to the decode\_frame\_common function in libavcodec/pngdec.c. | Merge in package |
| kernel | 3.10 | CVE-2017-15265 | Race condition in the ALSA subsystem in the Linux kernel before 4.13.8 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted /dev/snd/seq ioctl calls, related to sound/core/seq/seq\_clientmgr.c and sound/core/seq/seq\_ports.c. | <http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=71105998845fb012937332fe2e806d443c09e026> |
| kernel | 3.10 | 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. | <http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=5649645d725c73df4302428ee4e02c869248b4c5> |
| kernel | 3.10 | 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. | <http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=37863c43b2c6464f252862bf2e9768264e961678> |
| kernel | 3.10 | 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> |
| kernel | 3.10 | 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> |