

Product name	Confidentiality level
B311-521	CONFIDENTIAL
Product version	Total 7 pages
V1.0	

B311-521 Firmware Release Notes

V1.1

Prepared by	B311-521 Team	Date	2020-03-12
Reviewed by	B311-521 Team	Date	2020-03-12
Approved by	B311-521 Team	Date	2020-03-12



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2019-9-11	1.0	B311-521 10.0.2.1(H190SP6C00)	The 1 st Version	B311-521 Team
2019-10-16	1.1	B311-521 10.0.2.1(H190SP9C00)	The 2 st Version	B311-521 Team
2019-10-21	1.2	B311-521 10.0.2.1(H190SP11C00)	The 3 st Version	B311-521 Team
2019-11-6	1.3	B311-521 10.0.2.1(H190SP13C00)	The 4 st Version	B311-521 Team
2019-11-13	1.4	B311-521 10.0.2.1(H190SP14C00)	The 5 st Version	B311-521 Team
2019-11-19	1.5	B311-521 10.0.2.1(H190SP15C00)	The 6 st Version	B311-521 Team
2020-03-12	1.6	B311-521 10.0.2.1(H690SP3C00)	The 7 st Version	B311-521 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	3Firmware	5
3.1	Version Description	5
3.2	Firmware Specifications	5
3.3	Improvement in the Previous Version	5
3.4	Known Limitations and Issues	5
4	WebUI/HiLink	6
4.1	Version Description	6
4.2	WebUI/HiLink Specifications	6
4.3	Improvement in the Previous Version	6
4.4	Known Limitations and Issues	6
5	Software Vulnerabilities Fixes	7

1 Main Feature

Form Factor	Size: 180*126*18/36mm White
Features	LTE Cat4: 150Mbps/50 Mbps@ 00MBW LTE: B2/4/5/7/28/66 UMTS: B2/4/5 GSM: NA LTE transmit power 23dBm LTE Receiving sensitivity Confirm to 3GPP Requirements

2 Hardware

2.1 Version Description

Hardware Version:	WL6B311M VER.A
Platform & Chipset:	Balong V700R11C70B190

2.2 Hardware Specifications

Item	Specifications
Technical standard	• IEEE 802.11 b/g/n, 2.4GHz(2*2) 2.4G 2*2: 802.11b/g/n : 17/16/16dBm+-3dBm
Operating frequency	LTE Cat4: 150Mbps/50 Mbps@ 00MBW LTE: B2/4/5/7/28/66 UMTS: B2/4/5 GSM: NA LTE transmit power 23dBm LTE Receiving sensitivity Confirm to 3GPP Requirements
Maximum power consumption	12 W
Power supply	AC: 100 V ~ 240 V
	DC: 12 V, 1 A
External interfaces	1*RJ45 (GE) 1*RJ11 1*SMA 1*Power 1*SIM card slot (2FF)
Button	Power switch, Reset switch, WPS switch
Dimensions (D × W × H)	180*126*18/36mm White
Temperature	Operating: 0℃ to +40℃

Item	Specifications
	Storage: -40℃ to +70℃
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 3Firmware

3.1 Version Description

Firmware Version: 10.0.2.1(H690SP3C00)
Baseline information Balong V700R11C70B185

3.2 Firmware Specifications

Item	Specifications

3.3 Improvement in the Previous Version

Index	Case ID	Issue Description
NA	NA	To optimize the rf NV

3.4 Known Limitations and Issues

Index	Case ID	Issue Description
1		



2		
---	--	--

4 WebUI/HiLink

4.1 Version Description

WebUI/HiLink Version: WEBUI 10.0.2.1(W2SP2C03)

4.2 WebUI/HiLink Specifications

Item	Specifications

4.3 Improvement in the Previous Version

Index	Case ID	Issue Description

4.4 Known Limitations and Issues

Index	Case ID	Issue Description



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	Impact Description
expat	2.2.6	CVE-2018-20843	In libexpat in Expat before 2.2.7, XML input including XML names that contain a large number of colons could make the XML parser consume a high amount of RAM and CPU resources while processing (enough to be usable for denial-of-service attacks).	https://github.com/libexpat/libexpat/pull/262/commits/11f8838bf99ea0a6f0b76f9760c43704d00c4ff6
Kernel	4.4	CVE-2019-12456	An issue was discovered in the MPT3COMMAND case in _ctl_ioctl_main in drivers/scsi/mpt3sas/mpt3sas_ctl.c in the Linux kernel through 5.1.5. It allows local users to cause a denial of service or possibly have unspecified other impact by changing the value of ioc_number between two kernel reads of that value, aka a "double fetch" vulnerability	https://git.kernel.org/pub/scm/linux/kernel/git/mkp/scsi.git/commit/?h=5.3/scsi-queue&id=86e5aca7fa2927060839f3e3b40c8bd65a7e8d1e
Kernel	4.4	CVE-2019-11478	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service.	https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md
Kernel	4.4	CVE-2018-9422	In get_futex_key of futex.c, there is a use-after-free due to improper locking. This could lead to local escalation of privilege with no additional privileges needed. User interaction is not needed for exploitation	https://source.android.com/security/bulletin/2018-07-01



<i>Kernel</i>	<i>4.4</i>	<i>CVE-2019-13272</i>	<i>In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic).</i>	<i>https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6994ee7b0053799d2e07cd140df6c2ea106c41ee</i>
---------------	------------	-----------------------	--	--