

Product name	Confidentiality level
E8372h-155	CONFIDENTIAL
Product version	Total 6 pages
V1.0	

E8372h-155 Firmware Release Notes

V1.0

Prepared by	qinlei qwx451290	Date	2017-5-26
Reviewed by		Date	
Approved by		Date	



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

Date	Revision version	FW-WebUI/Stick Version	Change Description	Author
2017-3-8	1.0	FW 21.325.03.00.00	First version	qinlei
2017-4-10		FW 21.326.03.00.00	Fixed Bug	qinlei
2017-4-28		FW 21.326.05.00.00	Fixed Bug	qinlei
2017-4-28		FW 21.326.07.00.00	Fixed Bug	Qinlei
2017-8-29		FW 21.328.01.00.00	Fixed Bug	Xiayichao
2017-11-1		FW 21.328.03.00.00	Fixed Bug	Xiayichao
2018-06-05		FW 21.331.01.00.00	MR Version	Xiayichao
2019-4-17		FW 21.335.01.00.00	MR Version	Xiayichao
2019-7-18		FW 21.335.03.00.00	MR Version	Xiayichao
2019-10-23		FW 21.335.05.00.00	MR Version	Xiayichao

Table of Contents

1	Main Features	4
2	Hardware	4
2.1	Hardware Specifications	4
3	Firmware	5
3.1	Version Description	5
3.2	Firmware Specifications	5
3.3	Improvement in the Previous Version	6
3.4	Known Limitations and Issues	6
4	Software Vulnerabilities Fixes	6

E8372h-155 Firmware Release Notes V1.0

1 Main Features

The E8372h-155 supports the following standards:

- LTE Mainstream Product
- CN and India
- Highlights:
- LTE/WiFi high speed share
- Support cat4
- Support 16 users online
- Hilink APP

2 Hardware

2.1 Hardware Specifications

Inofrmation		E8372h-155
Key Feature	state	USB Stick 30*94*14.6mm Weight:<35g
	Main feature	FDD LTE Cat4:150/50Mbps @20M BW HSPA+ 42/5.76,21/5.76 Mbps HSPA:14/5.76,7.2/5.76 Mbps WLAN:IEEE802.11b/g/n, up to16 devices Receive Diversity, Data service, Internal antenna, Hilink APP, Web UI online update LTE B1,B3,B8,B38,B39,B40(2300-2398),B41(2535-2655) UMTS B1, B8 TD-SCDMA B34,39



		battery: none
		RTL8189 WiFi 1*1; SIM card slot 3*LED lights: LTE(3G)/WiFi/SMS
		Chipset: Balong V711 +ATPV2
		OS: 1) Windows7, Windows 8, Windows 8.1, Win10 Note: Does not support Windows RT 2) Mac OS X10.7, 10.8, 10.9, 10.10 and 10.11 with latest upgrades

3 Firmware

3.1 Version Description

Firmware Version: 21.335.05.00.00

Baseline information Balong V7R11 C30B335

3.2 Firmware Specifications

Firmware		
Item	Specifications	
Version	21.335.05.00.00	
Information	Platform	Balong V7R11
	Baseline	C30B331
	Feature	LTE Supported
	UMTS PS domain	<ul style="list-style-type: none">• Uplink: 384 kbit/s• Downlink: 384 kbit/s
	HSDPA	<ul style="list-style-type: none">• 14.4Mbit/s
	HSUPA	<ul style="list-style-type: none">• 5.76 Mbit/s
	HSPA+	<ul style="list-style-type: none">• 21.6Mbit/s
	DC HSPA+	<ul style="list-style-type: none">• Uplink:5.76 Mbit/s• Downlink:43.2Mbit/s
	LTE FDD	<ul style="list-style-type: none">• Uplink: 50Mbit/s• Downlink:150Mbit/s
SMS	<ul style="list-style-type: none">• SMS over SGs	
Operating System	<ul style="list-style-type: none">• Windows XP/Windows Vista/WIN 7/MAC/WIN8	



3.3 Improvement in the Previous Version

Index	Case ID	Issue Description
1		
2		

3.4 Known Limitations and Issues

Index	Case ID	Issue Description

4 WebUI/HiLink

4.1 Version Description

WebUI/HiLink Version: 21.100.52.01.03

4.2 WebUI/HiLink Specifications

Item	Specifications

4.3 Improvement in the Previous Version

Index	Case ID	Issue Description
WebUI Version		21.100.52.00.03
Previous WebUI Version		N/A
1		
2		
3		

4.4 Known Limitations and Issues

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



Index	Case ID	Issue Description
1	Unrealized Features	
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	Impact Description
linux_kernel	3.4.5	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	https://github.com/torvalds/linux/commit/1e38da300e1e395a15048b0af1e5305bd91402f6



			<i>file-descriptor operations that leverage improper might_cancel queueing.</i>	
<i>Google</i>	<i>#11 patch</i>	<i>CVE-2017-0841</i>	<i>In the utf16_to_utf8_length function of libutils, there could be an integer overflow leading to remote code execution.</i>	<i>Android ID:A-37723026,Impacted Module:System/Libutils.</i>
<i>Google</i>	<i>#11 patch</i>	<i>CVE-2017-0860</i>	<i>An app with SYSTEM_ALERT_WINDOW could use a collection of overlays to determine the user's keystrokes.</i>	<i>Android ID:A-31097064,Impacted Module:System/InputDispatcher.</i>
<i>Google</i>	<i>#11 patch</i>	<i>CVE-2016-2105</i>	<i>Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of</i>	<i>https://git.openssl.org/?p=openssl.git;a=commit;h=5b814481f3573fa9677f3a31ee51322e2a22ee6a</i>



			<i>binary data.</i>	
<i>Google</i>	<i>#11 patch</i>	<i>CVE-2016-2106</i>	<i>Integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.</i>	<i>https://www.freebsd.org/security/advisories/FreeBSD-SA-16:17.openssl.asc</i>
<i>linux kernel</i>	<i>4.4</i>	<i>CVE-2015-8966</i>	<i>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.</i>	<i>Merge the patch https://github.com/torvalds/linux/commit/76cc404bfdc0d419c720de4daaf2584542734f42</i>
<i>linux_kernel</i>	<i>3.4.5</i>	<i>CVE-2017-17806</i>	<i>The HMAC implementation (crypto/hmac.c) in the Linux kernel before</i>	<i>https://github.com/torvalds/linux/commit/af3ff8045bbf3e32f1a448542e73ab4c8ceb6f1</i>



			<i>4.14.8 does not validate that the underlying cryptographic hash algorithm is unkeyed, allowing a local attacker able to use the AF_ALG-based hash interface (CONFIG_CRYPTO_USER_API_HASH) and the SHA-3 hash algorithm (CONFIG_CRYPTO_SHA3) to cause a kernel stack buffer overflow by executing a crafted sequence of system calls that encounter a missing SHA-3 initialization.</i>	
<i>linux_kernel</i>	<i>3.4.5</i>	<i>CVE-2017-17558</i>	<i>The usb_destro_y_configuration function in drivers/usb/core/config.c in the USB core subsystem in the Linux kernel through 4.14.5 does not consider the maximum</i>	<i>https://download.novell.com/Download?buildid=3RrCrytYPvM~</i>



			<i>number of configurations and interfaces before attempting to release resources, which allows local users to cause a denial of service (out-of-bounds write access) or possibly have unspecified other impact via a crafted USB device.</i>	
		<i>CVE-2017-17712</i>	<i>The raw_sendmsg() function in net/ipv4/rw.c in the Linux kernel through 4.14.6 has a race condition in inet->hdrincl that leads to uninitialized stack pointer usage; this allows a local user to execute code and gain privileges.</i>	<i>https://github.com/torvalds/linux/commit/8f659a03a0ba9289b9aeb9b4470e6fb263d6f483</i>
<i>linux_kernel</i>	<i>3.4.5</i>	<i>CVE-2019-11477</i>	<i>Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segsize value was subject to</i>	<i>https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md</i>



			<i>an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78c</i> <i>ff.</i>	
--	--	--	--	--

6 Accessory Product from other Vendor

7 Others

8 Reference