

Product name	Confidentiality level
E8372h	CONFIDENTIAL
Product version	Total 8 pages
V1.1	

E8372h Firmware Release Notes

V1.1

Prepared by	V7R11 team	Date	2016-09-19
Reviewed by	V7R11 team	Date	2016-09-19
Approved by		Date	



Huawei Technologies Co., Ltd.

All rights reserved

Revision Record

Date	Revision version	FW-WebUI/Stick Version	Change Description	Author
2016-09-19	1.0	FW 21.321.01.00.00	First version	V7R11 team
2017-3-16	1.1	FW21.323.01.00.00	MR version	liuming
2017-8-01	1.2	FW21.327.01.00.00	MR version	liuming
2017-9-18	1.3	FW21.328.01.00.00	MR version	Xiayichao
2017-10-24	1.4	FW21.328.03.00.00	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	5
3.1	Known Limitations and Issues	6
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
6	Accessory Product from other Vendor	7
6.1	Known Limitations and Issues	8
7	Others	8
8	Reference	8



E8372h Firmware Release Notes V1.1

1 Main Features

The E8372h supports the following standards:

- 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
- microSD Card Slot (Up to 32G)
- Data and SMS Service
- Plug and play
- Standard USB interface
- CSFB

2 Hardware

2.1 Hardware Specifications

Item	Specifications
Hardware Version	<ul style="list-style-type: none">● CL1E8372HM
Technical standard	<ul style="list-style-type: none">● LTE 3GPP R9● HSPA+/UMTS: 3GPP R99/R5/R6/R7/R8● GSM/GPRS/EDGE: 3GPP R99
External interfaces	USB: Type A with standard USB 2.0 High speed interface
	LED: indicating the status of the Data Card
	SD card: standard TF card interface
	SIM/USIM card: standard 6-pin SIM card interface
	RF interface: external RF interface
Maximum power consumption	≤ 3.5 W
Power supply	5V
Dimensions (D × W × H)	About 94mm(D) × 30mm(W) × 14mm (H)
Weight	≤ 50g



Item	Specifications
Temperature	<ul style="list-style-type: none">Operating: -10°C to +40°CStorage: -20°C to +70°C
Humidity	5% to 95%
Base Information	<ul style="list-style-type: none">Plug and play (PnP)
	<ul style="list-style-type: none">Standard USB 2.0 High Speed interface, auto installation, convenient for use
Note: 3GPP = The 3rd Generation Partnership Project TS = Technical Specification LED = Light-Emitting Diode SIM = Subscriber Identity Module USIM = UMTS Subscriber Identity Module	

3 Firmware

3.1 Version Description

Firmware Version:	21.328.03.00.00
Baseline information	Balong V7R11 C30B328

3.2 Firmware Specifications

Firmware	
Item	Specifications
Version	21.328.03.00.00

3.3 Improvement in the Previous Version

Index	Case ID	Issue Description
Firmware Version		21.328.03.00.00
Previous Firmware Version		21.328.01.00.00
1	NA	[v711 common problem] Repair Google Patch #11 vulnerabilities CVE-2017-0427
2		
3		
4		
5		



3.1 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: 17.100.19.00.03

4.2 WebUI/HiLink Specifications

Item	Specifications

4.3 Improvement in the Previous Version

Index	Case ID	Issue Description
WebUI Version		17.100.19.00.03
Previous WebUI Version		17.100.18.01.03
1	New Features	
2		
3		

4.4 Known Limitations and Issues

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	Solution
linux_kernel	3.10	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.	http://www.securityfocus.com/bid/96071

6 Accessory Product from other Vendor

Version Description

Accessory Product Version:



6.1 Known Limitations and Issues

7 Others

8 Reference