Product name	Confidentiality level
E303h	CONFIDENTIAL
Product version	Total 8 pages
V1.0	

E303h Release Notes

V1.0

Prepared by	E303h Team	Date	2015-11-28
Reviewed by	E303h Team	Date	2015-11-28
Approved by	E303h Team	Date	2015-11-28

HUAWEI

Huawei Technologies Co., Ltd.

Revision Record

Date	Revision version	FW Version	Change Description	Author
2015-11-28	1.0	21.318.35.00.00	The 1st Version	E303h Team

Table of Contents

E303h Release Notes V1.0

Abbreviations	Description
3GPP	The 3rd Generation Partnership Project
TS	Technical Specification
SIM	Subscriber Identity Module
LED	Light-Emitting Diode
USIM	UMTS Subscriber Identity Module

1 Main Features

The E303h supports the following standards:

- HSDPA packet data service of up to 7.2 Mbit/s
- HSUPA packet data service of up to 5.76 Mbit/s
- WCDMA PS domain data service of up to 384 Kbit/s
- EDGE packet data service of up to 236.8 Kbit/s
- GPRS packet data service of up to 85.6 Kbit/s
- SMS based on CS/Packet Switched (PS) domain of GSM and WCDMA
- Plug and play (PnP)
- USSD Service
- Micro Secure Digital Memory Card up to 32GB

2 Hardware

2.1 Version Description

Hardware Version:	CH1E3531SM
Platform & Chipset:	Chipset:Balong V3R3

2.2 Hardware Specification

Item	Specifications
Technical standard	● WCDMA/HSDPA ● HSUPA ● GSM/GPRS/EGPRS
Operating frequency	E303h-1: W2100 MHz E303h-2: W2100/W900 MHz E303h-03: W2100/W1900 MHz E303h-6: W2100/W1900/W850 MHz
	EDGE/GPRS/GSM: 1900/1800/900/850 MHz
Internal memory	128 MB Flash, 64 MB Memory

Item	Specifications
Maximum transmitter power	HSDPA/HSUPA/ WCDMA: +22 dBm (Power Class 3)
	GSM/GPRS 850/900 MHz: +32 dBm (Power Class 4)
	GSM/GPRS 1800 MHz/1900 MHz: +29 dBm (Power Class 1)
	EDGE 850/900MHz: +26 dBm (Power Class E2)
	EDGE 1800MHz/1900MHz: +25 dBm (Power Class E2)
Maximum power consumption	≤2.5 W
External Interfaces	USB interface: USB 2.0 high-speed interface
	LED: indicating the status of the network
	SIM/USIM card: standard 6-pin SIM card interface
	SD card interface: Standard micro SD card interface
Static Receiver Sensitivity	HSUPA/HSDPA/UMTS 2100/1900/900/850 MHz: compliant with 3GPP TS 25.101(R6)
	GSM/GPRS/EDGE 850/900/1800/1900 MHz: compliant with 3GPP TS 05.05 (R99)
Power supply	5 V / 500 mA
Dimensions (W × D × H)	85.5 mm x 27 mm x 12.1 mm
Weight	< 30 g
Temperature	Operating: -10℃ to +45℃
	Storage: -20℃ to +70℃
Humidity	5% to 95%

2.3 Improvement in the Previous Version

Index	Case ID	Issue Description
NA		

2.4 Known Limitations and Issues

Index	Case ID	Issue Description
NA		

3 Firmware

3.1 Version Description

Firmware Version:	21.318.35.00.00
Baseline information :	BalongV3R3C10

3.2 Firmware Specifications

Item	Description
Data service	GPRS: ● Uplink: 85.6 kbit/s ● Downlink: 85.6 kbit/s EDGE: ● Uplink: 236.8 kbit/s ● Downlink: 236.8 kbit/s WCDMA PS domain: ● Uplink: 384 kbit/s ● Downlink: 384 kbit/s HSDPA: ● 7.2 Mbit/s HSUPA: ● 5.76 Mbit/s
SMS	Based on CS domain/PS domain of GSM and WCDMA

3.3 Improvement in the Previous Version

Index	Case ID	Issue Description
NA		

3.4 Known Limitations and Issues

Index	Case ID	Issue Description
NA		

4 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	2.6.35	CVE-2014-3535	include/linux/netdevice.h in the Linux kernel before 2.6.36 incorrectly uses macros for netdev_printk and its related logging implementation, which allows remote attackers to cause a denial of service (NULL	Merge the patches

			pointer dereference and system crash) by sending invalid packets to a VxLAN interface	