

Product name	Confidentiality level
E3372h-320	CONFIDENTIAL
Product version	Total 11 pages
V1.0	

HUAWEI E3372h-320 11.0.1.1(H697SP3C00)

Release Notes V1.0

Prepared by	E3372h-320 Team	Date	2021/6/5
-------------	-----------------	------	----------



Huawei Technologies Co., Ltd.



Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2019-9-25	1.0	E3372h-320 10.0.3.1(H190SP1C00)	ST	E3372h-320 Team
2019-9-25	1.0	E3372h-320 10.0.3.1(H190SP2C00)	V2-2	E3372h-320 Team
2019-10-25	1.0	E3372h-320 10.0.3.1(H190SP3C00)	TR4	E3372h-320 Team
2019-11-08	1.0	E3372h-320 10.0.3.1 (H191SP6C00)	VN1	E3372h-320 Team
2019-11-21	1.0	E3372h-320 10.0.3.1 (H191SP7C00)	TR4A	E3372h-320 Team
2019-12-03	1.0	E3372h-320 10.0.3.1 (H192SP14C00)	VN2	E3372h-320 Team
2019-12-21	1.0	E3372h-320 10.0.3.1 (H192SP16C00)	VN2-2	E3372h-320 Team
2019-12-25	1.0	E3372h-320 10.0.3.1 (H192SP17C00)	TR6	E3372h-320 Team
2020-1-7	1.0	E3372h-320 10.0.3.1 (H192SP19C00)	TR6	E3372h-320 Team
2020-1-15	1.0	E3372h-320 10.0.3.1 (H192SP20C00)	TR6	E3372h-320 Team
2020-3-9	1.0	E3372h-320 10.0.3.1 (H192SP21C00)	TR6-MR	E3372h-320 Team
2020-7-14	1.0	E3372h-320 10.0.5.1 (H195SP23C00)	TR6-MR	E3372h-320 Team
2020-10-14	1.0	E3372h-320 11.0.1.1 (H697SP1C00)	MR	E3372h-320 Team
2021-6-5	1.0	E3372h-320 11.0.1.1 (H697SP3C00)	MR	E3372h-320 Team

Table of Contents

1	Main Features	4
2	Hardware	4
2.1	Version Description	4
2.2	Hardware Specifications	4
3	Firmware	5
3.1	Version Description	5
3.2	Firmware Specifications	5
4	WebUI/HiLink	5
4.1	Version Description	5
4.2	WebUI Specifications	6
5	Software Vulnerabilities Fixes	6
6	Accessory Product from other Vendor	9
6.1	Known Limitations and Issues	10
7	Others	10
8	Reference	10



E3372h-320 11.0.1.1(H697SP3C00) V1.0 Release Notes

1 Main Features

The E3372h supports the following standards:

- LTE FDD data service of up to DL150Mbit/s/UL50Mbit/s
- DC-HSPA+ data service of up to 42Mbit/s
- HSPA+ data service of up to 21Mbit/s (64QAM)
- HSDPA data service of up to 14.4 Mbit/s
- HSUPA data service up to 5.76 Mbit/s
- WCDMA data service of up to 384kbit/s
- GPRS packet data service of up to 85.6kbit/s
- LTE/UMTS/GSM SMS over SGs service
- Support PnP, Plug and Play
- Windows 7, Windows 8, Windows 8.1, Win10(Does not support Windows RT),
Mac OS x 10.9~10.15 with latest upgrades

2 Hardware

2.1 Version Description

Hardware Version:	CL4E3372HM Ver.A
Platform & Chipset:	Balong V7R11,

2.2 Hardware Specifications

Item	Specifications	
Technical standard	LTE/WCDMA/HSDPA/HSUPA/HSPA+/DC-HSPA+/GSM/GPRS/EDGE	
Operating frequency	LTE: B1/B3/B7/B8/B20/B28 DC-HSPA+/HSPA+/HSPA/UMTS: B1/B8 EDGE/GPRS/GSM: B2/B3/B5/B8	
External interfaces	One USB 2.0 High Speed (Type A)	
	One mini-SIM card interface	
	Five TS-5 External antenna interface	
LED	Indicating the status of the 2G/3G/4G	
Maximum transmitter power	LTE	+23dBm (Power Class 3)
	WCDMA/HSPA/HSPA+/DC-HSPA+	+24dBm (Power Class 3)

Item	Specifications	
	GSM/GPRS	B8 +33dBm (Power Class 4)
		B3 +30dBm (Power Class 1)
	EDGE	B8 +27dBm (Power Class E1)
		B3 +26dBm (Power Class E1)
Static receiver sensitivity	LTE FDD: Accorded with 3GPP TS 36.101(R9)	
	WCDMA/HSPA/HSPA+/DC-HSPA+: Compliant with 3GPP TS 25.101(R9)	
	GSM/GPRS/EDGE: Compliant with 3GPP TS 05.05 (R6)	
Maximum power consumption	<3.5W	
Dimensions (D × W × H)	88mm x 28mm x 11.5mm	
Weight	< 35g	
Temperature	• Operating: –10°C to +40°C • Storage: –20°C to +70°C	
Humidity	5% to 95%	

3 Firmware

3.1 Version Description

Firmware Version:	11.0.1.1(H697SP3C00)
Baseline information	Hi6921 V7R11

3.2 Firmware Specifications

Item	Specifications
NA	NA

4 WebUI/HiLink

4.1 Version Description

WebUI Version:	WEBUI 11.0.1.1(W13SP3C03)
----------------	---------------------------



4.2 WebUI Specifications

Item	Specifications
NA	NA

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	4.4.197	CVE-2021-26930	An issue was discovered in the Linux kernel 3.11 through 5.10.16, as used by Xen. To service requests to the PV backend, the driver maps grant references provided by the frontend. In this process, errors may be encountered. In one case, an error encountered earlier might be discarded by later processing, resulting in the caller assuming successful mapping, and hence subsequent operations trying to access space that wasn't mapped. In another case, internal state would be insufficiently updated, preventing safe recovery from the error. This affects drivers/block/xen-blkback/blkback.c.	Merge the patch
linux_kernel	4.4.197	CVE-2021-27365	An issue was discovered in the Linux kernel through 5.11.3. Certain iSCSI data structures do not have appropriate length constraints or checks, and can exceed the PAGE_SIZE value. An unprivileged user can send a Netlink message that is associated with iSCSI, and has a length up to the maximum length of a Netlink message.	Merge the patch
linux_kernel	4.4.197	CVE-2021-27364	An issue was discovered in the Linux kernel through 5.11.3. drivers/scsi/scsi_transport_iscsi.c is adversely affected by the ability of an unprivileged user to craft Netlink messages.	Merge the patch
linux_kernel	4.4.197	CVE-20	In drivers/target/target_core_xcopy.c in the	Merge the patch



<i>rnsl</i>		20-2837 4	<i>Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directory traversal in an XCOPY request, aka CID-2896c93811e3. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. The attacker gains control over file access because I/O operations are proxied via an attacker-selected backstore.</i>	
<i>linux_ke rnsl</i>	4.4.197	CVE-20 20-0466	<i>In do_epoll_ctl and ep_loop_check_proc of eventpoll.c, there is a possible use after free due to a logic error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-147802478References: Upstream kernel</i>	<i>Merge the patch</i>
<i>linux_ke rnsl</i>	4.4.197	CVE-20 19-1181 5	<i>An issue was discovered in rds_tcp_kill_sock in net/rds/tcp.c in the Linux kernel before 5.0.8. There is a race condition leading to a use-after-free, related to net namespace cleanup.</i>	<i>Merge the patch</i>
<i>linux_ke rnsl</i>	4.4.197	CVE-20 20-1435 1	<i>A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor perf events to corrupt memory and possibly escalate privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.</i>	<i>Merge the patch</i>
<i>linux_ke rnsl</i>	4.4.197	CVE-20 20-0444	<i>In audit_free_lsm_field of auditfilter.c, there is a possible bad kfree due to a logic error in audit_data_to_entry. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-150693166References: Upstream kernel</i>	<i>Merge the patch</i>
<i>linux_ke rnsl</i>	4.4.197	CVE-20 20-2956 9	<i>An issue was discovered in the Linux kernel through 5.10.1, as used with Xen through 4.14.x. The Linux kernel PV block backend expects the kernel thread handler to reset ring->xenblkd to NULL when stopped. However, the handler may not have time to run if the frontend quickly toggles between the states connect and disconnect. As a consequence, the block backend may re-use a pointer after it was freed. A misbehaving guest can trigger a dom0 crash by continuously connecting / disconnecting a block frontend. Privilege escalation and information leaks cannot be ruled out. This only affects systems with a Linux blkback.</i>	<i>Merge the patch</i>
<i>linux_ke rnsl</i>	4.4.197	CVE-20 20-2778 6	<i>A flaw was found in the Linux kernels implementation of MIDI, where an attacker with a local account and the permissions to issue an ioctl commands to midi devices, could trigger a use-after-free. A write to this specific memory while freed and before use could cause the flow of execution to change and possibly allow for memory corruption or privilege escalation.</i>	<i>Merge the patch</i>
<i>linux_ke</i>	4.4.197	CVE-20	<i>An out-of-bounds memory write flaw was found</i>	<i>Merge the patch</i>



<i>rnsl</i>		20-14305	<i>in how the Linux kernel's Voice Over IP H.323 connection tracking functionality handled connections on ipv6 port 1720. This flaw allows an unauthenticated remote user to crash the system, causing a denial of service. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.</i>	
<i>linux_ke rnsl</i>	4.4.197	CVE-2020-29374	<i>An issue was discovered in the Linux kernel before 5.7.3, related to mm/gup.c and mm/huge_memory.c. The get_user_pages (aka gup) implementation, when used for a copy-on-write page, does not properly consider the semantics of read operations and therefore can grant unintended write access, aka CID-17839856fd58.</i>	<i>Merge the patch</i>
<i>linux_ke rnsl</i>	4.4.197	CVE-2020-29370	<i>An issue was discovered in kmem_cache_alloc_bulk in mm/slub.c in the Linux kernel before 5.5.11. The slowpath lacks the required TID increment, aka CID-fd4d9c7d0c71.</i>	<i>Merge the patch</i>
<i>linux_ke rnsl</i>	4.4.197	CVE-2020-25705	<i>A flaw in the way reply ICMP packets are limited in the Linux kernel functionality was found that allows to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypassing source port UDP randomization. The highest threat from this vulnerability is to confidentiality and possibly integrity, because software that relies on UDP source port randomization are indirectly affected as well. Kernel versions before 5.10 may be vulnerable to this issue.</i>	<i>Merge the patch</i>
<i>openssl</i>	1.1.1f	CVE-2021-23841	<i>The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).</i>	<i>Merge the patch</i>
<i>openssl</i>	1.1.1f	CVE-2021-23840	<i>Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some</i>	<i>Merge the patch</i>

			cases where the input length is close to the maximum permissible length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).	
musl	1.2.0	CVE-2020-28928	In musl libc through 1.2.1, wcsnrtombs mishandles particular combinations of destination buffer size and source character limit, as demonstrated by an invalid write access (buffer overflow).	Merge the patch
Kernel	4.4	CVE-2019-15215	An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the drivers/media/usb/cpia2/cpia2_usb.c driver.	Merge the patch
Kernel	4.4	CVE-2019-15218	An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the drivers/media/usb/siano/smsusb.c driver.	Merge the patch
Kernel	4.4	CVE-2019-10142	A flaw was found in the Linux kernel's freescale hypervisor manager implementation, kernel versions 5.0.x up to, excluding 5.0.17. A parameter passed to an ioctl was incorrectly validated and used in size calculations for the page size calculation. An attacker can use this flaw to crash the system, corrupt memory, or create other adverse security affects.	Merge the patch
Kernel	4.4	CVE-2019-2054	In the seccomp implementation prior to kernel version 4.8, there is a possible seccomp bypass due to seccomp policies that allow the use of ptrace. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	Merge the patch
Kernel	4.4	CVE-2019-15211	An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the drivers/media/v4l2-core/v4l2-dev.c driver because drivers/media/radio/radio-raremono.c does not properly allocate memory.	Merge the patch

6 Accessory Product from other Vendor

Version Description

Accessory Product Version:



6.1 Known Limitations and Issues

7 Others

8 Reference