

Product name	Confidentiality level
E3372h-607	CONFIDENTIAL
Product version	Total 15 pages
V20.0	

# HUAWEI E3372hTCPU-22.333.01.00.00

## Release Notes V20.0

Prepared by	E3372h Team	Date	2018/10/10
-------------	-------------	------	------------



Huawei Technologies Co., Ltd.



## Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2014-9-30	1.0	FW 22.180.03.00.00	First version	E3372h Team
2014-10-11	2.0	FW 22.180.05.00.00	Second version	E3372h Team
2014-11-11	3.0	FW 22.180.09.00.00	Third version	E3372h Team
2014-12-18	4.0	FW 22.200.01.00.00	Fourth version	E3372h Team
2014-12-28	5.0	FW 22.200.03.00.00	Fifth version	E3372h Team
2015-1-22	6.0	FW 22.200.05.00.00	Sixth version	E3372h Team
2015-4-8	7.0	FW 22.200.07.00.00	Seventh version	E3372h Team
2015-4-18	8.0	FW 22.200.09.00.00	Eighth version	E3372h Team
2015-6-19	9.0	FW 22.200.13.00.00	nineth version	E3372h Team
2015-8-29	10.0	FW 22.200.15.00.00	Tenth version	E3372h Team
2015-11-24	11.0	FW 22.315.01.00.00	Eleventh version	E3372h Team
2016-4-13	12.0	FW 22.317.01.00.00	Twelfth version	E3372h Team
2016-10-31	13.0	FW 22.321.01.00.00	Thirteenth version	E3372h Team
2016-12-26	14.0	FW22.323.01.00.00	Fourteenth version	E3372h Team
2017-3-16	15.0	FW22.323.03.00.00	Fifteenth version	E3372h Team
2017-11-02	16.0	FW22.328.01.00.00	Sixteenth version	E3372h Team
2018-1-04	17.0	FW22.329.03.00.00	Seventeenth version	E3372h Team
2018-1-11	18.0	FW22.329.05.00.00	Eighteenth version	E3372h Team
2018-1-19	19.0	FW22.329.07.00.00	Nineteenth version	E3372h Team
2018-10-10	20.0	FW22.333.01.00.00	Twentieth version	E3372h 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	Firmware .....	5
3.1	Version Description .....	5
3.2	Firmware Specifications .....	6
3.3	Improvement in the Previous Version .....	6
3.4	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 .....	14
6.1	Known Limitations and Issues .....	15
7	Others .....	15
8	Reference .....	15



# HUAWEI E3372h TCPU-V200R002B333D01SP00C00 Release Notes V20.0

## 1 Main Features

The E3372h 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 Version Description

Hardware Version:	CL2E3372HM Ver.A (old PA) CL3E3372HM Ver.A(new PA)
Platform & Chipset:	Balong Hi6921 V7R11M,

### 2.2 Hardware Specifications

Item	Specifications
Hardware Version	<ul style="list-style-type: none"><li>● CL2E3372HM Ver.A (old PA)</li><li>● CL3E3372HM Ver.A(new PA)</li></ul>
Technical standard	<ul style="list-style-type: none"><li>● LTE 3GPP R9</li><li>● HSPA+/UMTS: 3GPP R99/R5/R6/R7/R8</li><li>● GSM/GPRS/EDGE: 3GPP R99</li></ul>
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



Item	Specifications
Maximum power consumption	≤ 3.5 W
Power supply	5V
Dimensions (D × W × H)	About 88mm(D) × 28mm(W) × 11.5mm (H)
Weight	≤ 25 g
Temperature	<ul style="list-style-type: none"><li>Operating: −10°C to +40°C</li><li>Storage: −20°C to +70°C</li></ul>
Humidity	5% to 95%
Base Information	<ul style="list-style-type: none"><li>Plug and play (PnP)</li></ul>
	<ul style="list-style-type: none"><li>Standard USB 2.0 High Speed interface, auto installation, convenient for use</li></ul>
<b>Note:</b> 3GPP = The 3rd Generation Partnership Project TS = Technical Specification LED = Light-Emitting Diode SIM = Subscriber Identity Module USIM = UMTS Subscriber Identity Module	

## 2.3 Improvements in the Previous Version

Index	Case ID	Issue Description
Hardware Version		CL2E3372HM Ver.A (old PA) CL3E3372HM Ver.A(new PA)
Previous Hardware Version		NA
NA	NA	NA

## 2.4 Known Limitations and Issues

Index	Case ID	Issue Description
NA	NA	NA

# 3 Firmware

## 3.1 Version Description

Firmware Version:	22.333.01.00.00
Baseline information	Hi6921 V7R11M



### 3.2 Firmware Specifications

Item	Specifications
NA	NA

### 3.3 Improvement in the Previous Version

Index	Case ID	Issue Description
Firmware Version		22.333.01.00.00
Previous Firmware Version		22.329.07.00.00
1	NA	NA

### 3.4 Known Limitations and Issues

Index	Case ID	Issue Description
1	NA	NA

## 4 WebUI/HiLink

### 4.1 Version Description

WebUI/HiLink Version: 17.100.20.03.03

### 4.2 WebUI/HiLink Specifications

Item	Specifications
NA	NA

### 4.3 Improvement in the Previous Version

Index	Case ID	Issue Description
WebUI Version		17.100.20.03.03
Previous WebUI Version		17.100.20.00.03
1	NA	NA

### 4.4 Known Limitations and Issues

Index	Case ID	Issue Description
1	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	Solution
Openssl	1.0.1p	CVE-2016-7056	An information disclosure vulnerability in OpenSSL & BoringSSL could enable a remote attacker to gain access to sensitive information. This issue is rated as Moderate due to details specific to the vulnerability.	Google 2017 5#
linux_kernel	3.4.5	CVE-2017-7184	The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not validate certain size data after an XFRM_MSG_NEWAE update, which allows local users to obtain root privileges or cause a denial of service (heap-based out-of-bounds access) by leveraging the CAP_NET_ADMIN capability, as demonstrated during a Pwn2Own competition at CanSecWest 2017 for the Ubuntu 16.10 linux-image-* package 4.8.0.41.52.	Google 2017 5# <a href="https://github.com/torvalds/linux/commit/f843ee6dd019bcece3e74e76ad9df0155655d0df">https://github.com/torvalds/linux/commit/f843ee6dd019bcece3e74e76ad9df0155655d0df</a>



linux_kernel	3.4.5	CVE-2012-2663	extensions/libxt_tcp.c in iptables through 1.4.21 does not match TCP SYN+FIN packets in --syn rules, which might allow remote attackers to bypass intended firewall restrictions via crafted packets. NOTE: the CVE-2012-6638 fix makes this issue less relevant.	<a href="http://www.spinics.net/lists/netfilter-devel/msg21248.html">http://www.spinics.net/lists/netfilter-devel/msg21248.html</a>
linux_kernel	3.4.5	CVE-2017-8890	The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.	<a href="http://git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=657831ffc38e30092a2d5f03d385d710eb88b09a">http://git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=657831ffc38e30092a2d5f03d385d710eb88b09a</a>
linux_kernel	3.4.5	CVE-2017-9074	The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls.	<a href="http://git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=2423496af35d94a87156b063ea5cedffc10a70a1">http://git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=2423496af35d94a87156b063ea5cedffc10a70a1</a>
linux_kernel	3.4.5	CVE-2017-7487	The ipxif_ioctl function in net/ipv4/af_ipx.c in the Linux kernel through 4.11.1 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a failed SIOCGIFADDR ioctl call for an IPX interface.	<a href="http://git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=ee0d8d8482345ff97a75a7d747efc309f13b0d80">http://git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=ee0d8d8482345ff97a75a7d747efc309f13b0d80</a>
linux_kernel	3.4.5	CVE-2017-9242	The __ip6_append_data function in net/ipv6/ip6_output.c in the Linux kernel through 4.11.3 is too late in checking whether an	<a href="http://git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=232cd35d0804cc241eb887bb8d4d9b3b">http://git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=232cd35d0804cc241eb887bb8d4d9b3b</a>





			overwrite of an skb data structure may occur, which allows local users to cause a denial of service (system crash) via crafted system calls.	9881c64a
linux_kernel	3.4.5	CVE-2016-4913	The <code>get_rock_ridge_filename</code> function in <code>fs/isofs/rock.c</code> in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing <code>\0</code> characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem.	<a href="http://git.kernel.org/cgiit/linux/kernel/git/torvalds/linux.git/commit/?id=99d825822eade8d827a1817357cbf3f889a552d6">http://git.kernel.org/cgiit/linux/kernel/git/torvalds/linux.git/commit/?id=99d825822eade8d827a1817357cbf3f889a552d6</a>
linux_kernel	3.4.5	CVE-2017-7472	The KEYS subsystem in the Linux kernel before 4.10.13 allows local users to cause a denial of service (memory consumption) via a series of <code>KEY_REQKEY_DEFL_THREAD_KEYRING</code> <code>keyctl_set_reqkey_keyring</code> calls.	<a href="http://git.kernel.org/cgiit/linux/kernel/git/torvalds/linux.git/commit/?id=c9f838d104fed6f2f61d68164712e3204bf5271b">http://git.kernel.org/cgiit/linux/kernel/git/torvalds/linux.git/commit/?id=c9f838d104fed6f2f61d68164712e3204bf5271b</a>
linux_kernel	3.4.5	CVE-2016-7117	Use-after-free vulnerability in the <code>__sys_recvmsg</code> function in <code>net/socket.c</code> in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a <code>recvmsg</code> system call that is mishandled during error processing.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=34b88a68f26a75e4fded796f1a49c40f82234b7d">https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=34b88a68f26a75e4fded796f1a49c40f82234b7d</a>
linux_kernel	3.4.5	CVE-2015-8966	<code>arch/arm/kernel/sys_oabi-compat.c</code> in the Linux kernel before 4.4 allows local users to gain privileges via a crafted (1) <code>F_OFD_GETLK</code> , (2) <code>F_OFD_SETLK</code> , or (3) <code>F_OFD_SETLKW</code> command in an <code>fcntl64</code> system call.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/</a>



linux_kernel	3.4.5	CVE-2017-9075	The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=fdcee2cbb8438702ea1b328fb6e0ac5e9a40c7f8">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=fdcee2cbb8438702ea1b328fb6e0ac5e9a40c7f8</a>
linux_kernel	3.4.5	CVE-2017-9076	The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=83eaddab4378db256d00d295bda6ca997cd13a52">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=83eaddab4378db256d00d295bda6ca997cd13a52</a>
linux_kernel	3.4.5	CVE-2017-9077	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=83eaddab4378db256d00d295bda6ca997cd13a52">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=83eaddab4378db256d00d295bda6ca997cd13a52</a>
linux_kernel	3.4.5	CVE-2016-9843	The crc32_big function in crc32.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving big-endian CRC calculation.	<a href="https://github.com/madler/zlib/commit/d1d577490c15a0c6862473d7576352a9f18ef811">https://github.com/madler/zlib/commit/d1d577490c15a0c6862473d7576352a9f18ef811</a>
linux_kernel	3.4.5	CVE-2015-5364	The (1) udp_recvmsg and (2) udpv6_recvmsg functions in the Linux kernel before 4.0.6 do not properly consider yielding a processor, which allows remote attackers to cause a denial of service (system hang) via incorrect checksums within a UDP packet flood.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=beb39db59d14990e401e235faf66a6b9b31240b0">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=beb39db59d14990e401e235faf66a6b9b31240b0</a>
linux_kernel	3.4.5	CVE-2016-9555	The sctp_sf_ootb function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk, which allows remote attackers to cause a denial of service (out-of-bounds slab access)	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=bf911e985d6bbaa328c20c3e05f4eb03de11fdd6">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=bf911e985d6bbaa328c20c3e05f4eb03de11fdd6</a>



			or possibly have unspecified other impact via crafted SCTP data.	
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 file-descriptor operations that leverage improper might_cancel queueing.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=1e38da300e1e395a15048b0af1e5305bd91402f6">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=1e38da300e1e395a15048b0af1e5305bd91402f6</a>
linux_kernel	3.4.5	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.	Google 2017 11# patch
linux_kernel	3.6.5	CVE-2017-17712	The raw_sendmsg() function in net/ipv4/raw.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.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8f659a03a0ba9289b9aeb9b4470e6fb263d6f483">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8f659a03a0ba9289b9aeb9b4470e6fb263d6f483</a>
linux_kernel	3.6.5	CVE-2017-16535	The usb_get_bos_descriptor function in drivers/usb/core/config.c in the Linux kernel before 4.13.10 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.	<a href="https://github.com/torvalds/linux/commit/1c0edc3633b56000e18d82fc241e3995ca18a69e">https://github.com/torvalds/linux/commit/1c0edc3633b56000e18d82fc241e3995ca18a69e</a>
linux_kernel	3.6.5	CVE-2017-16531	drivers/usb/core/config.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device, related to the	<a href="https://github.com/torvalds/linux/commit/bd7a3fe770ebd8391d1c7d072ff88e9e76d063eb">https://github.com/torvalds/linux/commit/bd7a3fe770ebd8391d1c7d072ff88e9e76d063eb</a>



			USB_DT_INTERFACE_AS SOCIATION descriptor.	
linux_kernel	3.6.5	CVE-2017-1000111	Linux kernel: heap out-of-bounds in AF_PACKET sockets. This new issue is analogous to previously disclosed CVE-2016-8655. In both cases, a socket option that changes socket state may race with safety checks in packet_set_ring. Previously with PACKET_VERSION. This time with PACKET_RESERVE. The solution is similar: lock the socket for the update. This issue may be exploitable, we did not investigate further. As this issue affects PF_PACKET sockets, it requires CAP_NET_RAW in the process namespace. But note that with user namespaces enabled, any process can create a namespace in which it has CAP_NET_RAW.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c27927e372f0785f3303e8fad94b85945e2c97b7">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c27927e372f0785f3303e8fad94b85945e2c97b7</a>
linux_kernel	3.6.5	CVE-2016-10088	Both damn things interpret userland pointers embedded into the payload; worse, they are actually traversing those. Leaving aside the bad API design, this is very much <code>_not_</code> safe to call with <code>KERNEL_DS</code> . Bail out early if that happens.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=128394eff343fc6d2f32172f03e24829539c5835">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=128394eff343fc6d2f32172f03e24829539c5835</a>
linux_kernel	3.6.5	CVE-2014-2523	net/netfilter/nf_conntrack_proto_dccp.c in the Linux kernel through 3.13.6 uses a DCCP header pointer incorrectly, which allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a DCCP packet that triggers a call to the (1) <code>dccp_new</code> , (2) <code>dccp_packet</code> , or (3) <code>dccp_error</code> function.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b22f5126a24b3b2f15448c3f2a254fc10cbc2b92">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b22f5126a24b3b2f15448c3f2a254fc10cbc2b92</a>



linux_kernel	3.6.5	CVE-2017-17712	The raw_sendmsg() function in net/ipv4/raw.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.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8f659a03a0ba9289b9aeb9b4470e6fb263d6f483">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8f659a03a0ba9289b9aeb9b4470e6fb263d6f483</a>
linux_kernel	3.4.5	CVE-2015-8966	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.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/</a>
linux_kernel	3.4.5	CVE-2016-7117	Use-after-free vulnerability in the __sys_recvmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmsg system call that is mishandled during error processing.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=34b88a68f26a75e4fdeb796f1a49c40f82234b7d">https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux-stable.git/commit/?id=34b88a68f26a75e4fdeb796f1a49c40f82234b7d</a>
linux_kernel	3.4.5	CVE-2017-17806	The HMAC implementation (crypto/hmac.c) in the Linux kernel before 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.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=af3ff8045bbf3e32f1a448542e73abb4c8ceb6f1">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=af3ff8045bbf3e32f1a448542e73abb4c8ceb6f1</a>
linux_kernel	3.4.5	CVE-2017-17558	The usb_destroy_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 number of configurations and interfaces before attempting to release resources, which allows local users to cause a denial	<a href="https://www.spinics.net/lists/linux-usb/msg163644.html">https://www.spinics.net/lists/linux-usb/msg163644.html</a>



			of service (out-of-bounds write access) or possibly have unspecified other impact via a crafted USB device.	
linux_kernel	3.4.5	CVE-2017-13246	In csum_partial_copy_fromiovecend of iovector.c, an offset of zero can be specified even when there are no iovs on the stack, causing an out of bounds read from a kernel stack buffer. This could lead to information disclosure.	Google 2018 2# patch
linux_kernel	3.6.5	CVE-2018-6927	The futex_requeue function in kernel/futex.c in the Linux kernel before 4.14.15 might allow attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact by triggering a negative wake or requeue value.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=fbe0e839d1e22d88810f3ee3e2f1479be4c0aa4a">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=fbe0e839d1e22d88810f3ee3e2f1479be4c0aa4a</a>
linux_kernel	3.4.5	CVE-2018-13053	The alarm_timer_nsleep function in kernel/time/alarmtimer.c in the Linux kernel through 4.17.3 has an integer overflow via a large relative timeout because ktime_add_safe is not used.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/tip/tip.git/commit/?id=5f936e19cc0ef97dbe3a56e9498922ad5ba1edef">https://git.kernel.org/pub/scm/linux/kernel/git/tip/tip.git/commit/?id=5f936e19cc0ef97dbe3a56e9498922ad5ba1edef</a>
linux_kernel	3.4.5	CVE-2018-1068	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged user to arbitrarily write to a limited range of kernel memory.	<a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b71812168571fa55e44cdd0254471331b9c4c4c6">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b71812168571fa55e44cdd0254471331b9c4c4c6</a>

## 6 Accessory Product from other Vendor

### Version Description

Accessory Product Version:



## **6.1 Known Limitations and Issues**

## **7 Others**

## **8 Reference**