

Product name	Confidentiality level
E5577Cs-603	CONFIDENTIAL
Product version	Total 17 pages
V6.0	

HUAWEI E5577Cs-603TCPU-V200R001B329D01SP00C00

Release Notes V6.0

Prepared by	E5577Cs-603 Team	Date	2018/3/16
-------------	------------------	------	-----------



Huawei Technologies Co., Ltd.



Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2015/4/11	1.0	FW 21.200.03.00.00 WEBUI_17.100.11.00.03	The 1 st Version	E5577Cs-603 Team
2015/5/5	2.0	FW 21.200.05.00.00 WEBUI_17.100.11.00.03	The 2 st Version	E5577Cs-603 Team
2015/5/19	3.0	FW 21.200.07.00.00 WEBUI_17.100.11.00.03	The 3 st Version	E5577Cs-603 Team
2016/9/6	4.0	FW 21.319.01.00.00 WEBUI_17.100.15.02.03	The 4 st Version	E5577Cs-603 Team
2017/10/26	5.0	FW 21.328.01.00.00 WEBUI_17.100.19.02.03	The 5 st Version	E5577Cs-603 Team
2018/3/16	6.0	FW 21.329.01.00.00 WEBUI_17.100.20.00.03	The 6 st Version	E5577Cs-603 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	5
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	6
	CVE-2016-4569	10
	CVE-2016-2108	11
6	Accessory Product from other Vendor	17
6.1	Known Limitations and Issues	17
7	Others.....	17
8	Reference	17



HUAWEI E5577Cs-603TCPU-V200R001B329D01SP00C00 Release Notes V6.0

1 Main Features

The E5577Cs-603 supports the following features:

- *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*
- *Data and SMS Service*
- *WEB UI, Auto connect*
- *Plug and play*
- *Standard USB2.0*
- *Support WiFi 2.4GHz*

2 Hardware

2.1 Version Description

Hardware Version:	CL3E5573SM06 Ver.A
Platform & Chipset:	Balong Hi6921 V7R11M, RTL8189

2.2 Hardware Specifications

Item	Specifications	
Technical Standard	3GPP	R99/R5/R6/R7/R8/R9
	IEEE	802.11b/g/n
Operating Frequency	LTE	TDD B40;FDD B3
	UMTS	B1
Maximum Transmitter Power	LTE	+23dBm (Class 3)
	UMTS	+24dBm (Class 3)
Maximum Power Consumption	3.5W	
Memory	128M NAND Flash, 128M DDR	
WLAN Rate	802.11b: 11Mbit/s, 5.5Mbit/s, 2Mbit/s, 1Mbit/s 802.11g: 54Mbit/s, 48Mbit/s, 36Mbit/s, 24Mbit/s, 18Mbit/s, 12Mbit/s, 9Mbit/s, 6Mbit/s 802.11n: MCS0-MCS7(WiFi 1x1), MCS0-MCS15(WiFi 2x2)	
External Interfaces	USB: Standard USB2.0	
	LCD	
	SIM/USIM card: 6pin, 1.8/3V	



	Standard microSD card interface
Display	LCD
Keys	1 Power, 1 Reset, 1 Menu
Antenna	Internal
Static Receiver Sensitivity	Compliant with 3GPP TS 36.101(R9) for LTE, TS 25.101(R8) for UMTS.
Battery	1500mAh
Dimensions (D × W × H)	96.8*58*13.5 mm
Weight	<85g(include Battery)
Ambient Temperature	0-35°C
Humidity	5%-95%

2.3 Improvements in the Previous Version

Index	Case ID	Issue Description
Hardware Version		CL3E5573SM06 Ver.A
Previous Hardware Version		NA

2.4 Known Limitations and Issues

Index	Case ID	Issue Description
NA		NA

3 Firmware

3.1 Version Description

Firmware Version: 21.329.01.00.00
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		21.329.01.00.00
Previous Version	Firmware	21.328.01.00.00

3.4 Known Limitations and Issues

Index	Case ID	Issue Description
1	Unrealized Features	NA

4 WebUI/HiLink

4.1 Version Description

WebUI/HiLink Version: 17.100.20.00.03

4.2 WebUI/HiLink Specifications

Item	Specifications
NA	NA

4.3 Improvement in the Previous Version

Index	Case ID	Issue Description
WebUI Version		17.100.20.00.03
Previous Version	WebUI	17.100.19.02.03
1	New Features	NA

4.4 Known Limitations and Issues

Index	Case ID	Issue Description
1	Unrealized Features	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	3.4.5	CVE-2016-5195	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=19be0eaffa3ac7d8eb6784ad9bdbc7d67ed8e619
Android	4.4.4, 5.0.2, 5.1.1	CVE-2016-6700	The entry->uncompressedSize and entry->data values could be modified to a position beyond the bounds of the buffer, which could lead to the possibility of code execution. The fix is designed to add bounds checks and reject zip file entries that have no filenames.	https://source.android.com/security/bulletin/2016-11-01.html
linux_kernel	3.10, 3.18	CVE-2016-6828	When the tcp_sendmsg function allocates a fresh and empty skb, it puts it at the tail of the write queue. On a failure condition, a dangling pointer is left leading to a potential use-after-free vulnerability. The fix is designed to set the highest_sack variable to null to prevent the potential use-after-free vulnerability.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=bb1fcca22492109be12640d49f5ea5a544c6bb4
linux_kernel	3.10, 3.18	CVE-2016-7910	There is a failure condition that can lead to a potential use-after-free vulnerability. The fix is designed to set the private pointer to NULL to prevent the potential use-after-free vulnerability.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=77da160530dd1dc94f6ae15a981f24e5f0021e84
linux_kernel	3.10, 3.18	CVE-2016-7911	There is a race condition accessing task->io_context	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=77da160530dd1dc94f6ae15a981f24e5f0021e84



			that can potentially lead to a use-after-free vulnerability. The fix is designed to add locking to prevent the potential use-after-free vuln	rvals/linux.git/commit/?id=8ba8682107ee2ca3347354e018865d8e1967c5f4
linux_kernel	3.10, 3.18	CVE-2015-8964	The line discipline drivers may mistakenly misuse ldisc-related fields when initializing leading to a potential information disclosure. The fix is designed to initialize relevant tty fields before instantiating the new line discipline to prevent the potential information disclosure.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=dd42bf1197144ede075a9d4793123f7689e164bc
linux_kernel	3.18	CVE-2016-6753	The format specifier %p can leak kernel addresses while not valuing the kptr_restrict system settings. The fix is designed to use %pK instead of %p, which also evaluates whether kptr_restrict is set.	https://source.android.com/security/bulletin/2016-11-01.html
linux_kernel	3.4, 3.10, 3.18	CVE-2014-9529	There is a race condition in the key_gc_unused_keys function in security/keys/gc.c file, in the Linux kernel through 3.18.2, that allows local users to execute code in the kernel or possibly have unspecified other impact via keyctl commands that trigger access to a key structure member during garbage collection of a key. The fix is designed to put the key->user after the destroy callback is called to prevent the race condition. Link to publicly available patch: Upstream kernel fix	http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=a3a8784454692dd72e5d5d34dcdab17b4420e74c
linux_kernel	3.4, 3.10, 3.18	CVE-2016-4470	The key_reject_and_link function in the security/keys/key.c file, in the Linux kernel through 4.6.3, contains an error in which a key-lookup could fail and in an attempt to cache, the failed lookup may attempt to free memory that could still be in use, leading to a potential use-after-free vulnerability. The fix is designed to add an additional check condition to ensure the data structure is	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=38327424b40bcebe2de92d07312c89360ac9229a



			initialized and prevents the potential use-after-free vulnerability. Link to publicly available patch: Upstream kernel fix	
linux_kernel	3.4	CVE-2015-2922	The ndisc_router_discovery function in net/ipv6/ndisc.c in the Neighbor Discovery (ND) protocol implementation in the IPv6 stack in the Linux kernel before 3.19.6 allows remote attackers to reconfigure a hop-limit setting via a small hop_limit value in a Router Advertisement (RA) message.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=38327424b40bcebe2de92d07312c89360ac9229a
linux_kernel	3.4	CVE-2014-8173	The pmd_none_or_trans_huge_or_clear_bad function in include/asm-generic/pgtable.h in the Linux kernel before 3.13 on NUMA systems does not properly determine whether a Page Middle Directory (PMD) entry is a transparent huge-table entry, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted MADV_WILLNEED madvise system call that leverages the absence of a page-table lock.	https://github.com/torvalds/linux/commit/ee53664bda169f519ce3c6a22d378f0b946c8178
Android	4.4.4, 5.0.2, 5.1.1	CVE-2016-2842	The internal fmtstr function used in processing a "%s" format string in the BIO_*printf functions could overflow while calculating the length of a string and cause an out of bounds read when printing very long strings. Additionally, the internal doapr_outch function can attempt to write to an out of bounds memory location (at an offset from the NULL pointer) in the event of a memory allocation failure. The fix is designed to address these memory issues.	https://git.openssl.org/?p=openssl.git;a=commit;h=578b956fe741bf8e84055547b1e83c28dd902c73
linux_kernel	3.4, 3.10,	CVE-2016-3841	There is a race condition in	http://git.kernel.org/c



	3.18		<p>the kernel networking component that could lead to a use-after-free vulnerability.</p> <p>The fix is designed to add read-copy-update synchronization protection to prevent the race condition.</p> <p>Link to publicly available patch: Upstream kernel fix</p>	<p>git/linux/kernel/git/torvalds/linux.git/commit/?id=45f6fad84cc305103b28d73482b344d7f5b76f39</p>
linux_kernel	3.4, 3.10, 3.18	CVE-2016-4482	<p>The proc_connectinfo function in the drivers/usb/core/devio.c file, in the Linux kernel through 4.6, does not initialize a certain data structure, which could allow local users to obtain sensitive information from kernel stack memory via a crafted USBDEVFS_CONNECTINFO IOCTL call.</p> <p>The fix is designed to zero out the usbdevfs_connectinfo struct before using it so no sensitive information can be returned.</p> <p>Link to publicly available patch: Upstream kernel fix</p>	<p>http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=681fef8380eb818c0b845fca5d2ab1dcbab114ee</p>
linux_kernel	3.4, 3.10, 3.18	CVE-2016-4578	<p>sound/core/timer.c in the Linux kernel through 4.6 does not initialize certain r1 data structures, which allows local users to obtain sensitive information from kernel stack memory via crafted use of the ALSA timer interface, related to the (1) snd_timer_user_ccallback and (2) snd_timer_user_tinterrupt functions.</p>	<p>http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=9a47e9cff994f37f7f0dbd9ae23740d0f64f9fe6</p>
linux_kernel	3.4, 3.10, 3.18	CVE-2016-4569	<p>The snd_timer_user_params function in sound/core/timer.c in the Linux kernel through 4.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via</p>	<p>http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=cec8f96e49d9be372fdb0c3836dcf31ec71e457e</p>



			crafted use of the ALSA timer interface.	
OpenSSL	1.0.1o and 1.0.2	CVE-2016-2108	The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue.	https://git.openssl.org/?p=openssl.git;a=commit;h=3661bb4e7934668bd99ca777ea8b30eedfafa871
linux_kernel	3.4.5	CVE-2016-2493	The Broadcom Wi-Fi driver in Android before 2016-06-01 on Nexus 5, Nexus 6, Nexus 6P, Nexus 7 (2013), Nexus Player, and Pixel C devices allows attackers to gain privileges via a crafted application, aka internal bug 26571522.	Google 2016 5# https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2493
linux_kernel	All Linux version	CVE-2016-0774	The (1) pipe_read and (2) pipe_write implementations in fs/pipe.c in a certain Linux kernel backport in the linux package before 3.2.73-2+deb7u3 on Debian wheezy and the kernel package before 3.10.0-229.26.2 on Red Hat Enterprise Linux (RHEL) 7.1 do not properly consider the side effects of failed __copy_to_user_inatomic and __copy_from_user_inatomic calls, which allows local users to cause a denial of service (system crash) or possibly gain privileges via a crafted application, aka an "I/O vector array overrun." NOTE: this vulnerability exists because of an incorrect fix for CVE-2015-1805.	Google 2016 4# https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0774
linux_kernel	All Linux version	CVE-2016-2438	DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2016-2547, CVE-2016-2548. Reason: This candidate is a duplicate of CVE-2016-2547 and CVE-2016-2548. Notes: All CVE users should reference CVE-2016-2547 and/or CVE-2016-2548 instead of this candidate. All references and descriptions in this	Google 2016 4# https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2438



			candidate have been removed to prevent accidental usage.	
Android	4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1	CVE-2016-2447	DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2016-4477. Reason: This candidate is a reservation duplicate of CVE-2016-4477. Notes: All CVE users should reference CVE-2016-4477 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	Google 2016 4# http://source.android.com/security/bulletin/2016-05-01.html
linux_kernel	before 3.16	CVE-2015-1805	The (1) pipe_read and (2) pipe_write implementations in fs/pipe.c in the Linux kernel before 3.16 do not properly consider the side effects of failed __copy_to_user_inatomic and __copy_from_user_inatomic calls, which allows local users to cause a denial of service (system crash) or possibly gain privileges via a crafted application, aka an "I/O vector array overrun."	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=f0d1bec9d58d4c038d0ac958c9af82be6eb18045
linux_kernel	Linux kernel through 4.9.9	CVE-2017-5970	Technical details: The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP options. This is due to dropping dst when bad IP options were present which could lead to a NULL pointer dereference. Fix details: The fix is designed to only drop the dst packet if it's safe to do so.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=34b2cef20f19c87999fff3da4071e66937db9644
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	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=bf911e985d6bbaa328c20c3e05f4eb03de11fdd6



			a denial of service (out-of-bounds slab access) or possibly have unspecified other impact via crafted SCTP data.	
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.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=2423496af35d94a87156b063ea5cedffc10a70a1
linux_kernel	3.4.5	CVE-2017-7487	The ipxif_ioctl function in net/ipx/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.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=ee0d8d8482345ff97a75a7d747efc309f13b0d80
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 overwrite of an skb data structure may occur, which allows local users to cause a denial of service (system crash) via crafted system calls.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=232cd35d0804cc241eb887bb8d4d9b3b9881c64a
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.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=657831ffc38e30092a2d5f03d385d710eb88b09a
linux_kernel	3.4.5	CVE-2017-9075	The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=657831ffc38e30092a2d5f03d385d710eb88b09a



			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.	mit/?id=fdcee2cbb8438702ea1b328fb6e0ac5e9a40c7f8
linux_kernel	3.4.5	CVE-2017-9076	The dccp_v6_request_rcv_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.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=83eaddab4378db256d00d295bda6ca997cd13a52
linux_kernel	3.4.5	CVE-2017-9077	The tcp_v6_syn_rcv_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.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=83eaddab4378db256d00d295bda6ca997cd13a52
linux_kernel	3.4.5	CVE-2016-4913	The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing \0 characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=99d825822eade8d827a1817357c6bf3f889a552d6
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 KEY_REQKEY_DEFL_TH_READ_KEYRING keyctl_set_reqkey_keyring calls.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c9f838d104fed6f2f61d68164712e3204bf5271b
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)	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=76cc404bfdc0d419c720de4daaf2584542734f42



			F_OFD_SETLKW command in an fcntl64 system call.	
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.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=34b88a68f26a75e4fded796f1a49c40f82234b7d
linux_kernel	3.4.5	CVE-2017-0427	If a thread's logd.auditd is scheduled while the group_leader of the thread's group is killed, that leader may be freed before the logging is completed. This may lead to use-after-free and memory corruption in the kernel, and possible code execution.	Google 2017 11# https://source.android.com/security/bulletin/2017-02-01.html
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.	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=af3ff8045bbf3e32f1a448542e73abb4c8ceb6f1
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 of service (out-of-bounds write access) or possibly have unspecified other impact via a crafted USB device.	https://www.spinics.net/lists/linux-usb/msg163644.html



linux_kernel	3.4.5	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.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8f659a03a0ba9289b9aeb9b4470e6fb263d6f483
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 _not_ safe to call with KERNEL_DS. Bail out early if that happens.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=128394eff343fc6d2f32172f03e24829539c5835
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) dccp_new, (2) dccp_packet, or (3) dccp_error function.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b22f5126a24b3b2f15448c3f2a254fc10cbc2b92
linux_kernel	3.4.5	CVE-2016-6301	The recv_and_process_client_pkt function in networking/ntpd.c in busybox allows remote attackers to cause a denial of service (CPU and bandwidth consumption) via a forged NTP packet, which triggers a communication loop.	https://git.busybox.net/busybox/commit/?id=150dc7a2b483b8338a3e185c478b4b23ee884e71
linux_kernel	3.4.5	CVE-2017-16544	In the add_match function in libbb/lineedit.c in BusyBox through 1.27.2, the tab autocomplete feature of the shell, used to get a list of filenames in a directory, does not sanitize filenames and results in executing any escape sequence in the terminal. This could	https://git.busybox.net/busybox/commit/?id=c3797d40a1c57352192c6106cc0f435e7d9c11e8



			potentially result in code execution, arbitrary file writes, or other attacks.	
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.	https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c27927e372f0785f3303e8fad94b85945e2c97b7

6 Accessory Product from other Vendor

Version Description

Accessory Product Version:

6.1 Known Limitations and Issues

7 Others

8 Reference