

---

# **pi2-buster-armhf Documentation**

*Release 2020-04-21-1859*

**The edi-pi Project Team**

**Apr 21, 2020**



## CONTENTS:

<b>1</b>	<b>Setup</b>	<b>1</b>
<b>2</b>	<b>Versions</b>	<b>3</b>
<b>3</b>	<b>Changelog</b>	<b>9</b>
3.1	base-files . . . . .	9
3.2	e2fsprogs . . . . .	9
3.3	libcom-err2 . . . . .	9
3.4	libext2fs2 . . . . .	9
3.5	libgnutls30 . . . . .	10
3.6	libidn2-0 . . . . .	10
3.7	libpython3.7-minimal . . . . .	10
3.8	libpython3.7-stdlib . . . . .	10
3.9	libsasl2-2 . . . . .	11
3.10	libsasl2-modules-db . . . . .	11
3.11	libss2 . . . . .	11
3.12	libsystemd0 . . . . .	11
3.13	libudev1 . . . . .	12
3.14	linux-image-4.19.0-8-armmp-lpae . . . . .	12
3.15	linux-image-armmp-lpae . . . . .	110
3.16	openssh-client . . . . .	110
3.17	openssh-server . . . . .	110
3.18	openssh-sftp-server . . . . .	111
3.19	python-apt-common . . . . .	111
3.20	python3-apt . . . . .	111
3.21	python3.7 . . . . .	112
3.22	python3.7-minimal . . . . .	112
3.23	sudo . . . . .	112
3.24	systemd . . . . .	113
3.25	systemd-sysv . . . . .	113
3.26	udev . . . . .	113



---

**CHAPTER  
ONE**

---

**SETUP**

Component	Setup
Ansible	2.5.1
Configuration	pi2-buster-armhf
edi	1.5.1.dev34+g98d7a9c
Project SCM revision	062b5541843adf65eb0934b3267af86cc8191f42



VERSIONS

Package	Version
adduser	3.118
apt	1.8.2
base-files	10.3+deb10u3
base-passwd	3.5.46
bash	5.0-4
bsdutils	1:2.33.1-0.1
ca-certificates	20190110
coreutils	8.30-3
cpio	2.12+dfsg-9
dash	0.5.10.2-5
dbus	1.12.16-1
debconf	1.5.71
debian-archive-keyring	2019.1
debianutils	4.8.6.1
diffutils	1:3.7-3
dirmngr	2.2.12-1+deb10u1
distro-info-data	0.41+deb10u1
dmsetup	2:1.02.155-3
dosfstools	4.1-2
dpkg	1.19.7
dumb-init	1.2.2-1.1
e2fsprogs	1.44.5-1+deb10u3
edi-boot-shim	0.8.0+deb10
fdisk	2.33.1-0.1
findutils	4.6.0+git+20190209-2
firmware-brcm80211	1:20190114-1+rpt4
gcc-8-base	8.3.0-6
gnupg	2.2.12-1+deb10u1
gnupg-110n	2.2.12-1+deb10u1
gnupg-utils	2.2.12-1+deb10u1
gpg	2.2.12-1+deb10u1
gpg-agent	2.2.12-1+deb10u1
gpg-wks-client	2.2.12-1+deb10u1
gpg-wks-server	2.2.12-1+deb10u1
gpgconf	2.2.12-1+deb10u1
gpgsm	2.2.12-1+deb10u1
gpgv	2.2.12-1+deb10u1

Continued on next page

Table 2.1 – continued from previous page

Package	Version
grep	3.3-1
gzip	1.9-3
haveged	1.9.1-7
hostname	3.21
ifupdown	0.8.35
init-system-helpers	1.56+nmu1
initramfs-tools	0.133+deb10u1
initramfs-tools-core	0.133+deb10u1
iproute2	4.20.0-2
iputils-ping	3:20180629-2
isc-dhcp-client	4.4.1-2
iso-codes	4.2-1
klibc-utils	2.0.6-1
kmod	26-1
libacl1	2.2.53-4
libapparmor1	2.13.2-10
libapt-inst2.0	1.8.2
libapt-pkg5.0	1.8.2
libargon2-1	0~20171227-0.2
libassuan0	2.5.2-1
libattr1	1:2.4.48-4
libaudit-common	1:2.8.4-3
libaudit1	1:2.8.4-3
libblkid1	2.33.1-0.1
libbsd0	0.9.1-2
libbz2-1.0	1.0.6-9.2~deb10u1
libc-bin	2.28-10
libc6	2.28-10
libcap-ng0	0.7.9-2
libcap2	1:2.25-2
libcap2-bin	1:2.25-2
libcom-err2	1.44.5-1+deb10u3
libcryptsetup12	2:2.1.0-5+deb10u2
libdb5.3	5.3.28+dfsg1-0.5
libdbus-1-3	1.12.16-1
libdebconfclient0	0.249
libdevmapper1.02.1	2:1.02.155-3
libdns-export1104	1:9.11.5.P4+dfsg-5.1
libedit2	3.1-20181209-1
libelf1	0.176-1.1
libexpat1	2.2.6-2+deb10u1
libext2fs2	1.44.5-1+deb10u3
libfdisk1	2.33.1-0.1
libffi6	3.2.1-9
libgcc1	1:8.3.0-6
libgcrypt20	1.8.4-5
libgmp10	2:6.1.2+dfsg-4
libgnutls30	3.6.7-4+deb10u3
libgpg-error0	1.35-1

Continued on next page



Table 2.1 – continued from previous page

Package	Version
libgssapi-krb5-2	1.17-3
libhavege1	1.9.1-7
libhogweed4	3.4.1-1
libidn11	1.33-2.2
libidn2-0	2.0.5-1+deb10u1
libip4tc0	1.8.2-4
libisc-export1100	1:9.11.5.P4+dfsg-5.1
libiw30	30~pre9-13
libjson-c3	0.12.1+ds-2
libk5crypto3	1.17-3
libkeyutils1	1.6-6
libklibc	2.0.6-1
libkmod2	26-1
libkrb5-3	1.17-3
libkrb5support0	1.17-3
libksba8	1.3.5-2
libldap-2.4-2	2.4.47+dfsg-3+deb10u1
libldap-common	2.4.47+dfsg-3+deb10u1
liblz4-1	1.8.3-1
liblzma5	5.2.4-1
libmnl0	1.0.4-2
libmount1	2.33.1-0.1
libmpdec2	2.4.2-2
libncurses6	6.1+20181013-2+deb10u2
libncursesw6	6.1+20181013-2+deb10u2
libnettle6	3.4.1-1
libnl-3-200	3.4.0-1
libnl-genl-3-200	3.4.0-1
libnl-route-3-200	3.4.0-1
libnpth0	1.6-1
libp11-kit0	0.23.15-2
libpam-modules	1.3.1-5
libpam-modules-bin	1.3.1-5
libpam-runtime	1.3.1-5
libpam0g	1.3.1-5
libparted2	3.2-25
libpcre3	2:8.39-12
libpcsc-lite1	1.8.24-1
libprocps7	2:3.3.15-2
libpython3-stdlib	3.7.3-1
libpython3.7-minimal	3.7.3-2+deb10u1
libpython3.7-stdlib	3.7.3-2+deb10u1
libreadline7	7.0-5
libsasl2-2	2.1.27+dfsg-1+deb10u1
libsasl2-modules-db	2.1.27+dfsg-1+deb10u1
libseccomp2	2.3.3-4
libselinux1	2.8-1+b1
libsemanage-common	2.8-2
libsemanage1	2.8-2

Continued on next page

Table 2.1 – continued from previous page

Package	Version
libsepol1	2.8-1
libsmartcols1	2.33.1-0.1
libsqlite3-0	3.27.2-3
libss2	1.44.5-1+deb10u3
libssl1.1	1.1.1d-0+deb10u2
libstdc++6	8.3.0-6
libsystemd0	241-7~deb10u3
libtasn1-6	4.13-3
libtinfo6	6.1+20181013-2+deb10u2
libudev1	241-7~deb10u3
libunistring2	0.9.10-1
libuuid1	2.33.1-0.1
libwrap0	7.6.q-28
libxtables12	1.8.2-4
libzstd1	1.3.8+dfsg-3
linux-base	4.6
linux-image-4.19.0-8-armmp-lpae	4.19.98-1
linux-image-armmp-lpae	4.19+105+deb10u3
login	1:4.5-1.1
lsb-base	10.2019051400
lsb-release	10.2019051400
mawk	1.3.3-17+b3
mender-client	1.7.0-4+b12
mime-support	3.62
mount	2.33.1-0.1
ncurses-base	6.1+20181013-2+deb10u2
ncurses-bin	6.1+20181013-2+deb10u2
net-tools	1.60+git20180626.aebd88e-1
netbase	5.6
openssh-client	1:7.9p1-10+deb10u2
openssh-server	1:7.9p1-10+deb10u2
openssh-sftp-server	1:7.9p1-10+deb10u2
openssl	1.1.1d-0+deb10u2
parted	3.2-25
passwd	1:4.5-1.1
perl-base	5.28.1-6
pinentry-curses	1.1.0-2
procps	2:3.3.15-2
python-apt-common	1.8.4.1
python3	3.7.3-1
python3-apt	1.8.4.1
python3-minimal	3.7.3-1
python3.7	3.7.3-2+deb10u1
python3.7-minimal	3.7.3-2+deb10u1
readline-common	7.0-5
resolvconf	1.79
sed	4.7-1
sensible-utils	0.0.12
sudo	1.8.27-1+deb10u2

Continued on next page

Table 2.1 – continued from previous page

Package	Version
systemd	241-7~deb10u3
systemd-sysv	241-7~deb10u3
sysvinit-utils	2.93-8
tar	1.30+dfsg-6
tzdata	2019c-0+deb10u1
u-boot-tools	2019.01+dfsg-7
ucf	3.0038+nmu1
udev	241-7~deb10u3
util-linux	2.33.1-0.1
wireless-tools	30~pre9-13
wpa_supplicant	2:2.7+git20190128+0c1e29f-6+deb10u1
zlib1g	1:1.2.11.dfsg-1



## CHANGELOG

### 3.1 base-files

#### 3.1.1 10.3+deb10u3 - 01. February 2020

- Change `/etc/debian_version` to 10.3, for Debian 10.3 point release.

### 3.2 e2fsprogs

#### 3.2.1 1.44.5-1+deb10u3 - 09. January 2020

- Fix [CVE-2019-5188](#): potential stack underflow in `e2fsck` (Closes: [#948508](#))
- Fix use after free in `e2fsck` (Closes: [#948517](#))

### 3.3 libcom-err2

#### 3.3.1 1.44.5-1+deb10u3 - 09. January 2020

- Fix [CVE-2019-5188](#): potential stack underflow in `e2fsck` (Closes: [#948508](#))
- Fix use after free in `e2fsck` (Closes: [#948517](#))

### 3.4 libext2fs2

#### 3.4.1 1.44.5-1+deb10u3 - 09. January 2020

- Fix [CVE-2019-5188](#): potential stack underflow in `e2fsck` (Closes: [#948508](#))
- Fix use after free in `e2fsck` (Closes: [#948517](#))

## 3.5 libgnutls30

### 3.5.1 3.6.7-4+deb10u3 - 03. April 2020

- Non-maintainer upload by the Security Team.
- GNUTLS-SA-2020-03-31: dtls client hello: fix zeroed random (CVE-2020-11501) Fix a DTLS-protocol regression (caused by TLS1.3 support), since 3.6.3. The DTLS client would not contribute any randomness to the DTLS negotiation, breaking the security guarantees of the DTLS protocol. (Closes: #955556)

### 3.5.2 3.6.7-4+deb10u2 - 19. January 2020

- Fix parsing of certificates using RegisteredID Closes: #949293

## 3.6 libidn2-0

### 3.6.1 2.0.5-1+deb10u1 - 30. January 2020

- Non-maintainer upload by the Security Team.
- Fix free of random (stack) value in idn2\_to\_ascii\_4i()
- idn2\_to\_ascii\_4i(): Restrict output length to 63 (CVE-2019-18224) (Closes: #942895)
- Fail make if 'ronn' doesn't exist when building docs
- Fix generation of idn2.1 man page file
- Move texinfo from Build-Depends-Indep to Build-Depends (Closes: #949705)

## 3.7 libpython3.7-minimal

### 3.7.1 3.7.3-2+deb10u1 - 20. December 2019

- CVE-2019-9740
- CVE-2019-9947
- CVE-2019-9948
- CVE-2019-10160
- CVE-2019-16056
- CVE-2019-16935

## 3.8 libpython3.7-stdlib

### 3.8.1 3.7.3-2+deb10u1 - 20. December 2019

- CVE-2019-9740

- CVE-2019-9947
- CVE-2019-9948
- CVE-2019-10160
- CVE-2019-16056
- CVE-2019-16935

## 3.9 libsasl2-2

### 3.9.1 2.1.27+dfsg-1+deb10u1 - 19. December 2019

- Non-maintainer upload by the Security Team.
- Off-by-one in `_sasl_add_string` function (CVE-2019-19906) (Closes: #947043)

## 3.10 libsasl2-modules-db

### 3.10.1 2.1.27+dfsg-1+deb10u1 - 19. December 2019

- Non-maintainer upload by the Security Team.
- Off-by-one in `_sasl_add_string` function (CVE-2019-19906) (Closes: #947043)

## 3.11 libss2

### 3.11.1 1.44.5-1+deb10u3 - 09. January 2020

- Fix CVE-2019-5188: potential stack underflow in `e2fsck` (Closes: #948508)
- Fix use after free in `e2fsck` (Closes: #948517)

## 3.12 libsystemd0

### 3.12.1 241-7~deb10u3 - 29. January 2020

- core: set `fs.file-max` sysctl to `LONG_MAX` rather than `ULONG_MAX`. Since kernel 5.2 (but also stable kernels like 4.19.53) the kernel thankfully returns proper errors when we write a value out of range to the sysctl. Which however breaks writing `ULONG_MAX` to request the maximum value. Hence let's write the new maximum value instead, `LONG_MAX`. (Closes: #945018)
- core: change ownership/mode of the execution directories also for static users. This ensures that execution directories like `CacheDirectory` and `StateDirectory` are properly chowned to the user specified in `User=` before launching the service. (Closes: #919231)

## 3.13 libudev1

### 3.13.1 241-7~deb10u3 - 29. January 2020

- core: set fs.file-max sysctl to LONG\_MAX rather than ULONG\_MAX. Since kernel 5.2 (but also stable kernels like 4.19.53) the kernel thankfully returns proper errors when we write a value out of range to the sysctl. Which however breaks writing ULONG\_MAX to request the maximum value. Hence let's write the new maximum value instead, LONG\_MAX. (Closes: #945018)
- core: change ownership/mode of the execution directories also for static users. This ensures that execution directories like CacheDirectory and StateDirectory are properly chowned to the user specified in User= before launching the service. (Closes: #919231)

## 3.14 linux-image-4.19.0-8-armmp-lpae

### 3.14.1 4.19.98-1 - 26. January 2020

- New upstream stable update: <https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.88>
  - [arm64] clk: meson: gxbb: let sar\_adc\_clk\_div set the parent clock rate
  - ASoC: compress: fix unsigned integer overflow check
  - reset: Fix memory leak in reset\_control\_array\_put()
  - [armhf] clk: samsung: exynos5433: Fix error paths
  - [armel/marvell,armhf] ASoC: kirkwood: fix external clock probe defer
  - [armel/marvell,armhf] ASoC: kirkwood: fix device remove ordering
  - [armhf] clk: samsung: exynos5420: Preserve PLL configuration during suspend/resume
  - [x86] pinctrl: cherryview: Allocate IRQ chip dynamic
  - [armhf] dts: imx6qdl-sabreauto: Fix storm of accelerometer interrupts
  - reset: fix reset\_control\_ops kerneldoc comment
  - [armhf,arm64] clk: sunxi: Fix operator precedence in sunxi\_divs\_clk\_setup
  - [armhf] clk: sunxi-ng: a80: fix the zero'ing of bits 16 and 18
  - [armhf] dts: sun8i-a83t-tbs-a711: Fix WiFi resume from suspend
  - [ppc64el] bpf: Fix tail call implementation
  - idr: Fix integer overflow in idr\_for\_each\_entry
  - idr: Fix idr\_alloc\_u32 on 32-bit systems
  - [x86] resctrl: Prevent NULL pointer dereference when reading mondata
  - [armhf] clk: ti: dra7-atl-clock: Remove ti\_clk\_add\_alias call
  - [armhf] clk: ti: clkctrl: Fix failed to enable error with double udelay timeout
  - bridge: ebttables: don't crash when using dnat target in output chains
  - can: peak\_usb: report bus recovery as well
  - can: rx-offload: can\_rx\_offload\_queue\_tail(): fix error handling, avoid skb mem leak



- can: rx-offload: can\_rx\_offload\_offload\_one(): do not increase the skb\_queue beyond skb\_queue\_len\_max
- can: rx-offload: can\_rx\_offload\_offload\_one(): increment rx\_fifo\_errors on queue overflow or OOM
- can: rx-offload: can\_rx\_offload\_offload\_one(): use ERR\_PTR() to propagate error value in case of errors
- can: rx-offload: can\_rx\_offload\_irq\_offload\_timestamp(): continue on error
- can: rx-offload: can\_rx\_offload\_irq\_offload\_fifo(): continue on error
- [armhf] can: flexcan: increase error counters if skb enqueueing via can\_rx\_offload\_queue\_sorted() fails
- [arm64] watchdog: meson: Fix the wrong value of left time
- ceph: return -EINVAL if given fsc mount option on kernel w/o support
- net/fq\_impl: Switch to kvmalloc() for memory allocation
- mac80211: fix station inactive\_time shortly after boot
- block: drbd: remove a stray unlock in \_\_drbd\_send\_protocol()
- scsi: target/tcmu: Fix queue\_cmd\_ring() declaration
- scsi: lpfc: Fix kernel Oops due to null pring pointers
- scsi: lpfc: Fix dif and first burst use in write commands
- tracing: Lock event\_mutex before synth\_event\_mutex
- [armhf] dts: imx\*: Fix memory node duplication
- [armhf] dts: Fix hsi gdd range for omap4
- [arm64] mm: Prevent mismatched 52-bit VA support
- [arm64] smp: Handle errors reported by the firmware
- [armhf] bus: ti-sysc: Check for no-reset and no-idle flags at the child level
- [arm64] RDMA/hns: Fix the bug while use multi-hop of pbl
- [x86] RDMA/vmw\_pvrdma: Use atomic memory allocation in create AH
- [armhf] PM / AVS: SmartReflex: NULL check before some freeing functions is not needed
- xfs: zero length symlinks are not valid
- ACPI / LPSS: Ignore acpi\_device\_fix\_up\_power() return value
- scsi: lpfc: Enable Management features for IF\_TYPE=6
- scsi: qla2xxx: Fix NPIV handling for FC-NVMe
- scsi: qla2xxx: Fix for FC-NVMe discovery for NPIV port
- nvme: provide fallback for discard alloc failure
- [s390x] zcrypt: make sysfs reset attribute trigger queue reset
- crypto: user - support incremental algorithm dumps
- mwifiex: fix potential NULL dereference and use after free
- mwifiex: debugfs: correct histogram spacing, formatting
- brcmfmac: set F2 watermark to 256 for 4373
- brcmfmac: set SDIO F1 MesBusyCtrl for CYW4373

- rtl818x: fix potential use after free
- bcache: do not check if debug dentry is ERR or NULL explicitly on remove
- bcache: do not mark writeback\_running too early
- xfs: require both realtime inodes to mount
- nvme: fix kernel paging oops
- ubifs: Fix default compression selection in ubifs
- ubi: Put MTD device after it is not used
- ubi: Do not drop UBI device reference before using
- iwlfwif: move iwl\_nvm\_check\_version() into dvm
- iwlfwif: mvm: force TCM re-evaluation on TCM resume
- iwlfwif: pcie: fix erroneous print
- iwlfwif: pcie: set cmd\_len in the correct place
- [armhf,arm64] gpio: pca953x: Fix AI overflow on PCAL6524
- gpiolib: Fix return value of gpio\_to\_desc() stub if !GPIOLIB
- [x86] kvm: vmx: Set IA32\_TSC\_AUX for legacy mode guests
- [x86] Revert "KVM: nVMX: reset cache/shadows when switching loaded VMCS"
- [x86] Revert "KVM: nVMX: move check\_vmentry\_postreqs() call to nested\_vmx\_enter\_non\_root\_mode()"
- VSOCK: bind to random port for VMADDR\_PORT\_ANY
- [amd64] mmc: meson-gx: make sure the descriptor is stopped on errors
- [armhf] mtd: rawnand: sunxi: Write pageprog related opcodes to WCMD\_SET
- [armhf] usb: ehci-omap: Fix deferred probe for phy handling
- btrfs: Check for missing device before bio submission in btrfs\_map\_bio
- btrfs: fix ncopies raid\_attr for RAID56
- btrfs: dev-replace: set result code of cancel by status of scrub
- Btrfs: allow clear\_extent\_dirty() to receive a cached extent state record
- btrfs: only track ref\_heads in delayed\_ref\_updates
- [x86] HID: intel-ish-hid: fixes incorrect error handling
- serial: 8250: Rate limit serial port rx interrupts during input overruns
- [x86] kprobes/xen: blacklist non-attachable xen interrupt functions
- xen/pciback: Check dev\_data before using it
- kprobes: Blacklist symbols in arch-defined prohibited area
- [amd64] kprobes: Show x86-64 specific blacklisted symbols correctly
- [armhf] memory: omap-gpmc: Get the header of the enum
- net/mlx5: Continue driver initialization despite debugfs failure
- netfilter: nf\_nat\_sip: fix RTP/RTCP source port translations

- exofs\_mount(): fix leaks on failure exits
- bnxt\_en: Return linux standard errors in bnxt\_ethtool.c
- bnxt\_en: Save ring statistics before reset.
- bnxt\_en: query force speeds before disabling autoneg mode.
- [s390x] KVM: unregister debug feature on failing arch init
- dm flakey: Properly corrupt multi-page bios.
- gfs2: take jdata unstuff into account in do\_grow
- dm raid: fix false -EBUSY when handling check/repair message
- xfs: Align compat attrlist\_by\_handle with native implementation.
- xfs: Fix bulkstat compat ioctls on x32 userspace.
- IB/qib: Fix an error code in qib\_sdma\_verbs\_send()
- vxlan: Fix error path in \_\_vxlan\_dev\_create()
- [ppc64el] xmon: fix dump\_segments()
- drivers/regulator: fix a missing check of return value
- Bluetooth: hci\_bcm: Handle specific unknown packets after firmware loading
- RDMA/srp: Propagate ib\_post\_send() failures to the SCSI mid-layer
- scsi: qla2xxx: deadlock by configfs\_depend\_item
- scsi: csistor: fix incorrect dma device in case of vport
- brcmfmac: Fix access point mode
- ath6kl: Only use match sets when firmware supports it
- ath6kl: Fix off by one error in scan completion
- [ppc64el] perf: Fix unit\_sel/cache\_sel checks
- [ppc64el] prom: fix early DEBUG messages
- [ppc64el] mm: Make NULL pointer dereferences explicit on bad page faults.
- [ppc64el] vfio/spapr\_tce: Get rid of possible infinite loop
- [ppc64el] powernv/eeh/npu: Fix uninitialized variables in opal\_pci\_eeh\_freeze\_status
- drbd: ignore “all zero” peer volume sizes in handshake
- drbd: reject attach of unsuitable uuids even if connected
- drbd: do not block when adjusting “disk-options” while IO is frozen
- drbd: fix print\_st\_err()’s prototype to match the definition
- IB/rxe: Make counters thread safe
- bpf/cpumap: make sure frame\_size for build\_skb is aligned if headroom isn’t
- [armhf] regulator: tps65910: fix a missing check of return value
- [ppc64el] powerpc/pseries: Fix node leak in update\_lmb\_associativity\_index()
- net/netlink\_compat: Fix a missing check of nla\_parse\_nested
- net/net\_namespace: Check the return value of register\_pernet\_subsys()

- f2fs: fix block address for \_\_check\_sit\_bitmap
- f2fs: fix to dirty inode synchronously
- [armhf] net: dsa: bcm\_sf2: Propagate error value from mdio\_write
- atl1e: checking the status of atl1e\_write\_phy\_reg
- tipc: fix a missing check of genlmsg\_put
- net: marvell: fix a missing check of acpi\_match\_device
- ocfs2: clear journal dirty flag after shutdown journal
- vmscan: return NODE\_RECLAIM\_NOSCAN in node\_reclaim() when CONFIG\_NUMA is n
- mm/page\_alloc.c: free order-0 pages through PCP in page\_frag\_free()
- mm/page\_alloc.c: use a single function to free page
- mm/page\_alloc.c: deduplicate \_\_memblock\_free\_early() and memblock\_free()
- netfilter: nf\_tables: fix a missing check of nla\_put\_failure
- xprtrdma: Prevent leak of rprdma\_rep objects
- infiniband/qedr: Potential null ptr dereference of qp
- lib/genalloc.c: fix allocation of aligned buffer from non-aligned chunk
- lib/genalloc.c: use vzalloc\_node() to allocate the bitmap
- drivers/base/platform.c: kmemleak ignore a known leak
- lib/genalloc.c: include vmalloc.h
- mtd: Check add\_mtd\_device() ret code
- tipc: fix memory leak in tipc\_nl\_compat\_publ\_dump
- net/core/neighbour: tell kmemleak about hash tables
- [armhf,arm64] ata: ahci: mvebu: do Armada 38x configuration only on relevant SoCs
- PCI/MSI: Return -ENOSPC from pci\_alloc\_irq\_vectors\_affinity()
- net/core/neighbour: fix kmemleak minimal reference count for hash tables
- serial: 8250: Fix serial8250 initialization crash
- [armhf] gpu: ipu-v3: pre: don't trigger update if buffer address doesn't change
- sfc: suppress duplicate nvmem partition types in efx\_ef10\_mtd\_probe
- ip\_tunnel: Make none-tunnel-dst tunnel port work with lwtunnel
- decnet: fix DN\_IFREQ\_SIZE
- net/smc: prevent races between smc\_lgr\_terminate() and smc\_conn\_free()
- net/smc: don't wait for send buffer space when data was already sent
- mm/hotplug: invalid PFNs from pfn\_to\_online\_page()
- xfs: end sync buffer I/O properly on shutdown error
- net/smc: fix sender\_free computation
- blktrace: Show requests without sector
- net/smc: fix byte\_order for rx\_curs\_confirmed

- tipc: fix skb may be leaky in tipc\_link\_input
- sfc: initialise found bitmap in efx\_ef10\_mtd\_probe
- geneve: change NET\_UDP\_TUNNEL dependency to select
- net: fix possible overflow in \_\_sk\_mem\_raise\_allocated()
- net: ip\_gre: do not report erspan\_ver for gre or gretap
- net: ip6\_gre: do not report erspan\_ver for ip6gre or ip6gretap
- sctp: don't compare hb\_timer expire date before starting it
- bpf: decrease usercnt if bpf\_map\_new\_fd() fails in bpf\_map\_get\_fd\_by\_id()
- mmc: core: align max segment size with logical block size
- net: dev: Use unsigned integer as an argument to left-shift
- kvm: properly check debugfs dentry before using it
- bpf: drop refcount if bpf\_map\_new\_fd() fails in map\_create()
- [arm64] net: hns3: Change fw error code NOT\_EXEC to NOT\_SUPPORTED
- [arm64] net: hns3: fix PFC not setting problem for DCB module
- [arm64] net: hns3: fix an issue for hclgevf\_ae\_get\_hdev
- [arm64] net: hns3: fix an issue for hns3\_update\_new\_int\_gl
- [x86] iommu/amd: Fix NULL dereference bug in match\_hid\_uid
- apparmor: delete the dentry in aafs\_remove() to avoid a leak
- scsi: libsas: Support SATA PHY connection rate unmatched during discovery
- ACPI / APEI: Don't wait to serialise with oops messages when panic()ing
- ACPI / APEI: Switch estatus pool to use vmalloc memory
- [arm64] scsi: hisi\_sas: shutdown axi bus to avoid exception CQ returned
- scsi: libsas: Check SMP PHY control function result
- [arm64] RDMA/hns: Fix the bug with updating rq head pointer when flush cq
- [arm64] RDMA/hns: Bugfix for the scene without receiver queue
- [arm64] RDMA/hns: Fix the state of rereg mr
- [arm64] RDMA/hns: Use GFP\_ATOMIC in hns\_roce\_v2\_modify\_qp
- ASoC: rt5645: Headphone Jack sense inverts on the LattePanda board
- [ppc64el] pseries/dlpar: Fix a missing check in dlpar\_parse\_cc\_property() (CVE-2019-12614)
- xdp: fix cpumap redirect SKB creation bug
- mtd: Remove a debug trace in mtdpart.c
- [s390x] mm, gup: add missing refcount overflow checks on s390
- [armhf,arm64] usb: dwc2: use a longer core rest timeout in dwc2\_core\_reset()
- staging: rtl8192e: fix potential use after free
- staging: rtl8723bs: Drop ACPI device ids
- staging: rtl8723bs: Add 024c:0525 to the list of SDIO device-ids

- USB: serial: ftdi\_sio: add device IDs for U-Blox C099-F9P
- [x86] mei: bus: prefix device names on bus with the bus name
- [x86] mei: me: add comet point V device id
- thunderbolt: Power cycle the router if NVM authentication fails
- xfrm: Fix memleak on xfrm state destroy
- media: v4l2-ctrl: fix flags for DO\_WHITE\_BALANCE
- [arm64] net: macb: fix error format in dev\_err()
- pwm: Clear chip\_data in pwm\_put()
- macvlan: schedule bc\_work even if error
- net: psample: fix skb\_over\_panic
- openvswitch: fix flow command message size
- sctp: Fix memory leak in sctp\_sf\_do\_5\_2\_4\_dupcook
- slip: Fix use-after-free Read in slip\_open
- openvswitch: drop unneeded BUG\_ON() in ovs\_flow\_cmd\_build\_info()
- openvswitch: remove another BUG\_ON()
- tipc: fix link name length check
- sctp: cache netns in sctp\_ep\_common
- net: sched: fix *tc -s class show* no bstats on class with nolock subqueues
- [arm64] net: macb: add missed tasklet\_kill
- ext4: add more paranoia checking in ext4\_expand\_extra\_isize handling (CVE-2019-19767)
- [arm64] net: macb: Fix SUBNS increment and increase resolution
- [arm64] net: macb driver, check for SKBTX\_HW\_TSTAMP
- mtd: spi-nor: cast to u64 to avoid uint overflows
- tcp: exit if nothing to retransmit on RTO timeout
- HID: core: check whether Usage Page item is after Usage ID items
- [x86] platform: hp-wmi: Fix ACPI errors caused by too small buffer
- [x86] platform: hp-wmi: Fix ACPI errors caused by passing 0 as input size

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.89>

- rsi: release skb if rsi\_prepare\_beacon fails (CVE-2019-19071)
- [arm64] tegra: Fix 'active-low' warning for Jetson TX1 regulator
- usb: gadget: u\_serial: add missing port entry locking
- [arm64] tty: serial: msm\_serial: Fix flow control
- [armhf,arm64] serial: pl011: Fix DMA ->flush\_buffer()
- serial: serial\_core: Perform NULL checks for break\_ctl ops
- autofs: fix a leak in autofs\_expire\_indirect()
- [arm64] RDMA/hns: Correct the value of HNS\_ROCE\_HEM\_CHUNK\_LEN

- iwlfwifi: pcie: don't consider IV len in A-MSDU
- exportfs\_decode\_fh(): negative pinned may become positive without the parent locked
- audit\_get\_nd(): don't unlock parent too early
- xfrm: release device reference for invalid state
- sched/core: Avoid spurious lock dependencies
- perf/core: Consistently fail fork on allocation failures
- ALSA: pcm: Fix stream lock usage in snd\_pcm\_period\_elapsed()
- [armhf,arm64] drm/sun4i: tcon: Set min division of TCON0\_DCLK to 1.
- rsxx: add missed destroy\_workqueue calls in remove
- i2c: core: fix use after free in of\_i2c\_notify
- serial: core: Allow processing sysrq at port unlock time
- cxgb4vf: fix memleak in mac\_hlist initialization
- iwlfwifi: mvm: synchronize TID queue removal
- iwlfwifi: trans: Clear persistence bit when starting the FW
- iwlfwifi: mvm: Send non offchannel traffic via AP sta
- [armhf] 8813/1: Make aligned 2-byte getuser()/putuser() atomic on ARMv6+
- audit: Embed key into chunk
- netfilter: nf\_tables: don't use position attribute on rule replacement
- net/mlx5: Release resource on error flow
- [arm64] clk: sunxi-ng: a64: Fix gate bit of DSI DPHY
- ice: Fix NVM mask defines
- dlm: fix possible call to kfree() for non-initialized pointer
- [armhf] dts: exynos: Fix LDO13 min values on Odroid XU3/XU4/HC1
- [armhf,arm64] rtc: max77686: Fix the returned value in case of error in 'max77686\_rtc\_read\_time()'
- i40e: don't restart nway if autoneg not supported
- virtchnl: Fix off by one error
- [armhf] clk: rockchip: fix rk3188 sclk\_smc gate data
- [armhf] clk: rockchip: fix rk3188 sclk\_mac\_lbtst parameter ordering
- [armhf] dts: rockchip: Fix rk3288-rock2 vcc\_flash name
- dlm: fix missing idr\_destroy for recover\_idr
- [armhf,arm64] net: dsa: mv88e6xxx: Work around mv88e6161 SERDES missing MII\_PHYSID2
- [s390x] scsi: zfcp: update kernel message for invalid FCP\_CMND length, it's not the CDB
- [s390x] scsi: zfcp: drop default switch case which might paper over missing case
- [armhf] bus: ti-sysc: Fix getting optional clocks in clock\_roles
- [armhf] dts: imx6: RDU2: fix eGalax touchscreen node
- crypto: ecc - check for invalid values in the key verification test

- crypto: bcm - fix normal/non key hash algorithm failure
- [arm64] dts: zynqmp: Fix node names which contain “\_”
- [arm64] pinctrl: qcom: ssbi-gpio: fix gpio-hog related boot issues
- [arm\*] firmware: raspberrypi: Fix firmware calls with large buffers
- mm/vmstat.c: fix NUMA statistics updates
- [arm64] clk: rockchip: fix I2S1 clock gate register for rk3328
- [arm64] clk: rockchip: fix ID of 8ch clock of I2S1 for rk3328
- sctp: count sk\_wmem\_alloc by skb truesize in sctp\_packet\_transmit
- regulator: Fix return value of \_set\_load() stub
- USB: serial: f81534: fix reading old/new IC config
- xfs: extent shifting doesn't fully invalidate page cache
- net-next/hinic: fix a bug in set mac address
- net-next/hinic: fix a bug in rx data flow
- ice: Fix return value from NAPI poll
- ice: Fix possible NULL pointer de-reference
- iomap: FUA is wrong for DIO O\_DSYNCR writes into unwritten extents
- iomap: sub-block dio needs to zeroout beyond EOF
- iomap: dio data corruption and spurious errors when pipes fill
- iomap: readpages doesn't zero page tail beyond EOF
- iw\_cxgb4: only reconnect with MPAv1 if the peer aborts
- [mips\*/octeon] octeon-platform: fix typing
- net/smc: use after free fix in smc\_wr\_tx\_put\_slot()
- [armhf] dts: exynos: Use Samsung SoC specific compatible for DWC2 module
- media: pulse8-cec: return 0 when invalidating the logical address
- media: cec: report Vendor ID after initialization
- iwlfwifi: fix cfg structs for 22000 with different RF modules
- net/ipv6: re-do dad when interface has IFF\_NOARP flag change
- [x86] dmaengine: dw-dmac: implement dma protection control setting
- [armhf,arm64] usb: dwc3: debugfs: Properly print/set link state for HS
- [armhf,arm64] usb: dwc3: don't log probe deferrals; but do log other error codes
- ACPI: fix acpi\_find\_child\_device() invocation in acpi\_preset\_companion()
- f2fs: fix to account preflush command for noflush\_merge mode
- f2fs: fix count of seg\_freed to make sec\_freed correct
- f2fs: change segment to section in f2fs\_ioc\_gc\_range
- [armhf] dts: rockchip: Fix the PMU interrupt number for rv1108
- [armhf] dts: rockchip: Assign the proper GPIO clocks for rv1108



- f2fs: fix to allow node segment for GC by ioctl path
- nvme: Free ctrl device name on init failure
- dma-mapping: fix return type of dma\_set\_max\_seg\_size()
- [armhf] serial: imx: fix error handling in console\_setup
- [armhf] i2c: imx: don't print error message on probe defer
- [arm64] clk: meson: Fix GXL HDMI PLL fractional bits width
- [armhf,arm64] gpu: host1x: Fix syncpoint ID field size on Tegra186
- lockd: fix decoding of TEST results
- sctp: increase sk\_wmem\_alloc when head->truesize is increased
- [x86] iommu/amd: Fix line-break in error log reporting
- [armhf] dts: sun8i: a23/a33: Fix OPP DTC warnings
- [armhf] dts: sun8i: v3s: Change pinctrl nodes to avoid warning
- nfsd: fix a warning in \_\_cld\_pipe\_upcall()
- bpf: btf: implement btf\_name\_valid\_identifier()
- bpf: btf: check name validity for various types
- [armhf] OMAP1/2: fix SoC name printing
- [arm64] dts: meson-gxl-librettech-cc: fix GPIO lines names
- [arm64] dts: meson-gxbb-nanopi-k2: fix GPIO lines names
- [arm64] dts: meson-gxbb-odroidc2: fix GPIO lines names
- [arm64] dts: meson-gxl-khadas-vim: fix GPIO lines names
- net/x25: fix called/calling length calculation in x25\_parse\_address\_block
- net/x25: fix null\_x25\_address handling
- tcp: make tcp\_space() aware of socket backlog
- tcp: fix off-by-one bug on aborting window-probing socket
- tcp: fix SNMP under-estimation on failed retransmission
- tcp: fix SNMP TCP timeout under-estimation
- kbuild: fix single target build for external module
- mtd: fix mtd\_oobavail() incoherent returned value
- [arm64] clk: meson: meson8b: fix the offset of vid\_pll\_dco's N value
- [armhf,arm64] clk: sunxi-ng: h3/h5: Fix CSI\_MCLK parent
- [arm64] clk: qcom: Fix MSM8998 resets
- dlm: fix invalid cluster name warning
- net/mlx4\_core: Fix return codes of unsupported operations
- pstore/ram: Avoid NULL deref in ftrace merging failure path
- [mips\*/octeon] cvmx\_pko\_mem\_debug8: use oldest forward compatible definition
- nfsd: Return EPERM, not EACCES, in some SETATTR cases

- media: uvcvideo: Abstract streaming object lifetime
- [armhf] dts: sun8i: h3: Fix the system-control register range
- tty: Don't block on IO when ldisc change is pending
- media: stkwebcam: Bugfix for wrong return values
- sctp: frag\_point sanity check
- IB/hfi1: Ignore LNI errors before DC8051 transitions to Polling state
- IB/hfi1: Close VNIC sdma\_progress sleep window
- mlx4: Use snprintf instead of complicated strepy
- [armhf] dts: sunxi: Fix PMU compatible strings
- [armhf] dts: am335x-pdu001: Fix polarity of card detection input
- net: aquantia: fix RSS table and key sizes
- sched/fair: Scale bandwidth quota and period without losing quota/period ratio precision
- fuse: verify nlink
- fuse: verify attributes
- [x86] ALSA: hda/realtek - Enable internal speaker of ASUS UX431FLC
- [x86] ALSA: hda/realtek - Enable the headset-mic on a Xiaomi's laptop
- [x86] ALSA: hda/realtek - Dell headphone has noise on unmute for ALC236
- ALSA: pcm: oss: Avoid potential buffer overflows
- [x86] ALSA: hda - Add mute led support for HP ProBook 645 G4
- [x86] Input: synaptics - switch another X1 Carbon 6 to RMI/SMBus
- [x86] Input: synaptics-rmi4 - re-enable IRQs in f34v7\_do\_reflash
- [x86] Input: synaptics-rmi4 - don't increment rmiaddr for SMBus transfers
- [x86] Input: goodix - add upside-down quirk for Teclast X89 tablet
- Input: Fix memory leak in psxpad\_spi\_probe
- [i386] mm: Sync only to VMALLOC\_END in vmalloc\_sync\_all()
- [x86] PCI: Avoid AMD FCH XHCI USB PME# from D0 defect
- xfrm interface: fix memory leak on creation
- xfrm interface: avoid corruption on changelink
- xfrm interface: fix list corruption for x-netns
- xfrm interface: fix management of phydev
- CIFS: Fix NULL-pointer dereference in smb2\_push\_mandatory\_locks
- CIFS: Fix SMB2 oplock break processing
- tty: vt: keyboard: reject invalid keycodes
- can: slcan: Fix use-after-free Read in slcan\_open
- kernfs: fix ino wrap-around detection
- jbd2: Fix possible overflow in jbd2\_log\_space\_left()

- [arm64] drm/msm: fix memleak on release
- [i386] drm/i810: Prevent underflow in ioctl
- [armhf,arm64] KVM: vgic: Don't rely on the wrong pending table
- [x86] KVM: do not modify masked bits of shared MSRs
- [x86] KVM: fix presentation of TSX feature in ARCH\_CAPABILITIES
- [x86] KVM: Grab KVM's srcu lock when setting nested state
- crypto: af\_alg - cast ki\_complete ternary op to int
- [x86] crypto: ccp - fix uninitialized list head
- crypto: ecdh - fix big endian bug in ECC library
- crypto: user - fix memory leak in crypto\_report (CVE-2019-19062)
- mwifiex: update set\_mac\_address logic
- can: ucan: fix non-atomic allocation in completion handler
- RDMA/qib: Validate ->show()/store() callbacks before calling them
- iomap: Fix pipe page leakage during splicing
- thermal: Fix deadlock in thermal thermal\_zone\_device\_check
- vcs: prevent write access to vcsu devices (CVE-2019-19252)
- binder: Fix race between mmap() and binder\_alloc\_print\_pages()
- binder: Handle start==NULL in binder\_update\_page\_range()
- ALSA: hda - Fix pending unsol events at shutdown
- perf script: Fix invalid LBR/binary mismatch error
- splice: don't read more than available pipe space
- iomap: partially revert 4721a601099 (simulated directio short read on EFAULT)
- xfs: add missing error check in xfs\_prepare\_shift()
- ASoC: rsnd: fixup MIX kctrl registration
- [x86] KVM: fix out-of-bounds write in KVM\_GET\_EMULATED\_CPUID (CVE-2019-19332)
- net: qrtr: fix memort leak in qrtr\_tun\_write\_iter (CVE-2019-19079)
- appletalk: Fix potential NULL pointer dereference in unregister\_snap\_client (CVE-2019-19227)
- appletalk: Set error code if register\_snap\_client failed

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.90>

- usb: gadget: configfs: Fix missing spin\_lock\_init()
- [x86] usb: gadget: pch\_udc: fix use after free
- scsi: qla2xxx: Fix driver unload hang
- [arm64] media: venus: remove invalid compat\_ioctl32 handler
- USB: uas: honor flag to avoid CAPACITY16
- USB: uas: heed CAPACITY\_HEURISTICS
- usb: Allow USB device to be warm reset in suspended state

- staging: rtl8188eu: fix interface sanity check
- staging: rtl8712: fix interface sanity check
- staging: gigaset: fix general protection fault on probe
- staging: gigaset: fix illegal free on probe errors
- staging: gigaset: add endpoint-type sanity check
- usb: xhci: only set D3hot for pci device
- xhci: Fix memory leak in xhci\_add\_in\_port()
- xhci: Increase STS\_HALT timeout in xhci\_suspend()
- xhci: handle some XHCI\_TRUST\_TX\_LENGTH quirks cases as default behaviour.
- [armhf] dts: pandora-common: define wl1251 as child node of mmc3
- [x86] iio: imu: inv\_mpu6050: fix temperature reporting using bad unit
- USB: atm: ueagle-atm: add missing endpoint check
- USB: idmouse: fix interface sanity checks
- USB: serial: io\_edgeport: fix epic endpoint lookup
- usb: roles: fix a potential use after free
- USB: adutux: fix interface sanity check
- usb: core: urb: fix URB structure initialization function
- usb: mon: Fix a deadlock in usbmon between mmap and read
- tpm: add check after commands attribs tab allocation
- virtio-balloon: fix managed page counts when migrating pages between zones
- [armhf,arm64] usb: dwc3: gadget: Fix logical condition
- [armhf,arm64] usb: dwc3: ep0: Clear started flag on completion
- btrfs: check page->mapping when loading free space cache
- btrfs: use refcount\_inc\_not\_zero in kill\_all\_nodes
- Btrfs: fix metadata space leak on fixup worker failure to set range as delalloc
- Btrfs: fix negative subv\_writers counter and data space leak after buffered write
- btrfs: Avoid getting stuck during cyclic writebacks
- btrfs: Remove btrfs\_bio::flags member
- Btrfs: send, skip backreference walking for extents with many references
- btrfs: record all roots for rename exchange on a subvol
- rtlwifi: rtl8192de: Fix missing code to retrieve RX buffer address
- rtlwifi: rtl8192de: Fix missing callback that tests for hw release of buffer
- rtlwifi: rtl8192de: Fix missing enable interrupt flag
- ovl: fix corner case of non-unique st\_dev;st\_ino
- ovl: relax WARN\_ON() on rename to self
- [armhf] hwrng: omap - Fix RNG wait loop timeout

- dm writecache: handle REQ\_FUA
- dm zoned: reduce overhead of backing device checks
- workqueue: Fix spurious sanity check failures in destroy\_workqueue()
- workqueue: Fix pwq ref leak in rescuer\_thread()
- ASoC: rt5645: Fixed buddy jack support.
- ASoC: rt5645: Fixed typo for buddy jack support.
- ASoC: Jack: Fix NULL pointer dereference in snd\_soc\_jack\_report
- md: improve handling of bio with REQ\_PREFLUSH in md\_flush\_request()
- blk-mq: avoid sysfs buffer overflow with too many CPU cores
- cgroup: pids: use atomic64\_t for pids->limit
- ar5523: check NULL before memcpy() in ar5523\_cmd()
- [s390x] mm: properly clear \_PAGE\_NOEXEC bit when it is not supported
- media: cec.h: **CEC\_OP\_REC\_FLAG\_** values were swapped
- cpuidle: Do not unset the driver if it is there already
- erofs: zero out when listxattr is called with no xattr
- [x86] intel\_th: Fix a double put\_device() in error path
- [x86] intel\_th: pci: Add Ice Lake CPU support
- [x86] intel\_th: pci: Add Tiger Lake CPU support
- PM / devfreq: Lock devfreq in trans\_stat\_show
- [ppc64el] cpufreq: powernv: fix stack bloat and hard limit on number of CPUs
- ACPI / hotplug / PCI: Allocate resources directly under the non-hotplug bridge
- ACPI: OSL: only free map once in osl.c
- ACPI: bus: Fix NULL pointer check in acpi\_bus\_get\_private\_data()
- ACPI: PM: Avoid attaching ACPI PM domain to certain devices
- [arm64] pinctrl: armada-37xx: Fix irq mask access in armada\_37xx\_irq\_set\_type()
- [armhf] pinctrl: samsung: Add of\_node\_put() before return in error path
- [armhf] pinctrl: samsung: Fix device node refcount leaks in Exynos wakeup controller init
- [armhf] pinctrl: samsung: Fix device node refcount leaks in init code
- [armhf] mmc: host: omap\_hsmmc: add code for special init of wl1251 to get rid of pan-dora\_wl1251\_init\_card
- [armhf] dts: omap3-tao3530: Fix incorrect MMC card detection GPIO polarity
- ppdev: fix PPGETTIME/PPSETTIME ioctls
- [ppc64el] Allow 64bit VDSO \_\_kernel\_sync\_dicache to work across ranges >4GB
- [ppc64el] xive: Prevent page fault issues in the machine crash handler
- [ppc64el] Allow flush\_icache\_range to work across ranges >4GB
- [ppc64el] xive: Skip ioremap() of ESB pages for LSI interrupts

- video/hdmi: Fix AVI bar unpack
- quota: Check that quota is not dirty before release
- ext2: check err when partial != NULL
- quota: fix livelock in dquot\_writeback\_dquots
- ext4: Fix credit estimate for final inode freeing
- reiserfs: fix extended attributes on the root directory
- block: fix single range discard merge
- [s390x] scsi: zfcp: trace channel log even for FCP command responses
- scsi: qla2xxx: Fix DMA unmap leak
- scsi: qla2xxx: Fix hang in fcport delete path
- scsi: qla2xxx: Fix session lookup in qlt\_abort\_work()
- scsi: qla2xxx: Fix qla24xx\_process\_bidir\_cmd()
- scsi: qla2xxx: Always check the qla2x00\_wait\_for\_hba\_online() return value
- scsi: qla2xxx: Fix message indicating vectors used by driver
- scsi: qla2xxx: Fix SRB leak on switch command timeout
- xhci: make sure interrupts are restored to correct state
- usb: typec: fix use after free in typec\_register\_port()
- [armhf] omap: pdata-quirks: remove openpandora quirks for mmc3 and wl1251
- scsi: lpfc: Cap NPIV vports to 256
- scsi: lpfc: Correct code setting non existent bits in sli4 ABORT WQE
- scsi: lpfc: Correct topology type reporting on G7 adapters
- sch\_cake: Correctly update parent qlen when splitting GSO packets
- net/smc: do not wait under send\_lock
- [arm64] net: hns3: clear pci private data when unload hns3 driver
- [arm64] net: hns3: change hnae3\_register\_ae\_dev() to int
- [arm64] net: hns3: Check variable is valid before assigning it to another
- [arm64] scsi: hisi\_sas: send primitive NOTIFY to SSP situation only
- [arm64] scsi: hisi\_sas: Reject setting programmed minimum linkrate > 1.5G
- [x86] MCE/AMD: Turn off MC4\_MISC thresholding on all family 0x15 models
- [x86] MCE/AMD: Carve out the MC4\_MISC thresholding quirk
- ath10k: fix fw crash by moving chip reset after napi disabled
- [ppc64el] Fix vDSO clock\_getres()
- ext4: work around deleting a file with i\_nlink == 0 safely (CVE-2019-19447)
- mm/shmem.c: cast the type of unmap\_start to u64
- rtc: disable uie before setting time and enable after
- splice: only read in as much information as there is pipe buffer space

- ext4: fix a bug in ext4\_wait\_for\_tail\_page\_commit
- [armhf,arm64] mfd: rk808: Fix RK818 ID template
- mm, thp, proc: report THP eligibility for each vma
- [s390x] smp,vdso: fix ASCE handling
- blk-mq: make sure that line break can be printed
- workqueue: Fix missing kfree(rescuer) in destroy\_workqueue()
- perf callchain: Fix segfault in thread\_\_resolve\_callchain\_sample()
- gre: refetch erspan header from skb->data after pskb\_may\_pull()
- sunrpc: fix crash when cache\_head become valid before update
- net/mlx5e: Fix SFF 8472 eeprom length
- leds: trigger: netdev: fix handling on interface rename
- gfs2: fix glock reference problem in gfs2\_trans\_remove\_revoke
- of: overlay: add\_changeset\_property() memory leak
- kernel/module.c: wakeup processes in module\_wq on module unload
- cifs: Fix potential softlockups while refreshing DFS cache
- [x86] gpiolib: acpi: Add Terra Pad 1061 to the run\_edge\_events\_on\_boot\_blacklist
- raid5: need to set STRIPE\_HANDLE for batch head
- scsi: qla2xxx: Change discovery state before PLOGI
- [x86] iio: imu: mpu6050: add missing available scan masks
- idr: Fix idr\_get\_next\_ul race with idr\_remove
- of: unittest: fix memory leak in attach\_node\_and\_children

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.91>

- inet: protect against too small mtu values.
- mqprio: Fix out-of-bounds access in mqprio\_dump
- net: bridge: deny dev\_set\_mac\_address() when unregistering
- net: dsa: fix flow dissection on Tx path
- net: ethernet: ti: cpsw: fix extra rx interrupt
- net: sched: fix dump qlen for sch\_mq/sch\_mqprio with NOLOCK subqueues
- [arm64] net: thunderx: start phy before starting autonegotiation
- openvswitch: support asymmetric conntrack
- tcp: md5: fix potential overestimation of TCP option space
- tipc: fix ordering of tipc module init and exit routine
- net/mlx5e: Query global pause state before setting prio2buffer
- tcp: fix rejected syncookies due to stale timestamps
- tcp: tighten acceptance of ACKs not matching a child socket
- tcp: Protect accesses to .ts\_recent\_stamp with {READ,WRITE}\_ONCE()

- [arm64] Revert “arm64: preempt: Fix big-endian when checking preempt count in assembly”
- mmc: block: Make card\_busy\_detect() a bit more generic
- mmc: block: Add CMD13 polling for MMC IOCTLS with R1B response
- PCI/PM: Always return devices to D0 when thawing
- PCI: pciehp: Avoid returning prematurely from sysfs requests
- [x86] PCI: Fix Intel ACS quirk UPDCR register address
- PCI/MSI: Fix incorrect MSI-X masking on resume
- [arm64] PCI: Apply Cavium ACS quirk to ThunderX2 and ThunderX3
- [arm64] rpmsg: glink: Set tail pointer to 0 at end of FIFO
- [arm64] rpmsg: glink: Fix reuse intents memory leak issue
- [arm64] rpmsg: glink: Fix use after free in open\_ack TIMEOUT case
- [arm64] rpmsg: glink: Put an extra reference during cleanup
- [arm64] rpmsg: glink: Fix rpmsg\_register\_device err handling
- [arm64] rpmsg: glink: Don't send pending rx\_done during remove
- [arm64] rpmsg: glink: Free pending deferred work on remove
- cifs: smbd: Return -EAGAIN when transport is reconnecting
- cifs: smbd: Add messages on RDMA session destroy and reconnection
- cifs: smbd: Return -EINVAL when the number of iops exceeds SMBDIRECT\_MAX\_SGE
- cifs: Don't display RDMA transport on reconnect
- CIFS: Respect O\_SYNC and O\_DIRECT flags during reconnect
- CIFS: Close open handle after interrupted close
- [armhf] tegra: Fix FLOW\_CTLR\_HALT register clobbering by tegra\_resume()
- vfio/pci: call irq\_bypass\_unregister\_producer() before freeing irq
- dma-buf: Fix memory leak in sync\_file\_merge()
- [arm64] drm: meson: venc: cvbs: fix CVBS mode matching
- dm mpath: remove harmful bio-based optimization
- dm btree: increase rebalance threshold in \_\_rebalance2()
- scsi: iscsi: Fix a potential deadlock in the timeout handler
- scsi: qla2xxx: Change discovery state before PLOGI
- drm/radeon: fix r1xx/r2xx register checker for POT textures
- xhci: fix USB3 device initiated resume race with roothub autosuspend

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.92>

- af\_packet: set default value for tmo
- [amd64] fjes: fix missed check in fjes\_acpi\_add
- [arm64] net: hisilicon: Fix a BUG triggered by wrong bytes\_compl
- net: qlogic: Fix error paths in ql\_alloc\_large\_buffers()



- net: usb: lan78xx: Fix suspend/resume PHY register access error
- qede: Disable hardware gro when xdp prog is installed
- qede: Fix multicast mac configuration
- sctp: fully initialize v4 addr in some functions
- btrfs: don't double lock the subvol\_sem for rename exchange
- btrfs: do not call synchronize\_srcu() in inode\_tree\_del
- Btrfs: fix missing data checksums after replaying a log tree
- btrfs: send: remove WARN\_ON for readonly mount
- btrfs: abort transaction after failed inode updates in create\_subvol
- btrfs: skip log replay on orphaned roots
- btrfs: do not leak reloc root if we fail to read the fs root
- btrfs: handle ENOENT in btrfs\_uuid\_tree\_iterate
- Btrfs: fix removal logic of the tree mod log that leads to use-after-free issues
- ALSA: pcm: Avoid possible info leaks from PCM stream buffers
- ALSA: hda/ca0132 - Keep power on during processing DSP response
- ALSA: hda/ca0132 - Avoid endless loop
- ALSA: hda/ca0132 - Fix work handling in delayed HP detection
- [arm64,armhf] drm/panel: Add missing drm\_panel\_init() in panel drivers
- drm/amdgpu: grab the id mgr lock while accessing passid\_mapping
- spi: Add call to spi\_slave\_abort() function when spidev driver is released
- [x86] staging: rtl8192u: fix multiple memory leaks on error path
- staging: rtl8188eu: fix possible null dereference
- rtlwifi: prevent memory leak in rtl\_usb\_probe (CVE-2019-19063)
- libertas: fix a potential NULL pointer dereference
- ath10k: fix backtrace on coredump
- IB/iser: bound protection\_sg size by data\_sg size
- [arm64] media: venus: core: Fix msm8996 frequency table
- ath10k: fix offchannel tx failure when no ath10k\_mac\_tx\_frm\_has\_freq
- pinctrl: devicetree: Avoid taking direct reference to device name string
- [amd64] drm/amdkfd: fix a potential NULL pointer dereference
- [arm64] media: venus: Fix occasionally failures to suspend
- [armhf] hwrng: omap3-rom - Call clk\_disable\_unprepare() on exit only if not idled
- media: flexcop-usb: fix NULL-ptr deref in flexcop\_usb\_transfer\_init()
- [arm64,armhf] drm/bridge: dw-hdmi: Refuse DDC/CI transfers on the internal I2C controller
- block: Fix writeback throttling W=1 compiler warnings
- mwifiex: pcie: Fix memory leak in mwifiex\_pcie\_init\_evt\_ring (CVE-2019-19057)

- drm/drm\_vblank: Change EINVAL by the correct errno
- media: cx88: Fix some error handling path in 'cx8800\_initdev()'
- [armhf] media: ti-vpe: vpe: Fix Motion Vector vpdma stride
- [armhf] media: ti-vpe: vpe: fix a v4l2-compliance warning about invalid pixel format
- [armhf] media: ti-vpe: vpe: fix a v4l2-compliance failure about frame sequence number
- [armhf] media: ti-vpe: vpe: Make sure YUYV is set as default format
- [armhf] media: ti-vpe: vpe: fix a v4l2-compliance failure causing a kernel panic
- [armhf] media: ti-vpe: vpe: ensure buffers are cleaned up properly in abort cases
- [armhf] media: ti-vpe: vpe: fix a v4l2-compliance failure about invalid sizeimage
- [x86] syscalls/x86: Use the correct function type in SYSCALL\_DEFINE0
- [x86] mm: Use the correct function type for native\_set\_fixmap()
- ath10k: Correct error handling of dma\_map\_single()
- [arm64,armhf] drm/bridge: dw-hdmi: Restore audio when setting a mode
- perf report: Add warning when libunwind not compiled in
- usb: usbfs: Suppress problematic bind and unbind uevents.
- Bluetooth: missed cpu\_to\_le16 conversion in hci\_init4\_req
- Bluetooth: Workaround directed advertising bug in Broadcom controllers
- Bluetooth: hci\_core: fix init for HCI\_USER\_CHANNEL
- [x86] mce: Lower throttling MCE messages' priority to warning
- [x86] drm/gma500: fix memory disclosures due to uninitialized bytes
- rtl8xxxu: fix RTL8723BU connection failure issue after warm reboot
- ipmi: Don't allow device module unload when in use
- [x86] ioapic: Prevent inconsistent state when moving an interrupt
- md/bitmap: avoid race window between md\_bitmap\_resize and bitmap\_file\_clear\_bit
- [arm64] psci: Reduce the waiting time for cpu\_psci\_cpu\_kill()
- i40e: initialize ITRN registers with correct values
- net: phy: dp83867: enable robust auto-mdix
- [arm64,armhf] drm/tegra: sor: Use correct SOR index on Tegra210
- ACPI: button: Add DMI quirk for Medion Akoya E2215T
- RDMA/qedr: Fix memory leak in user qp and mr
- [arm64,armhf] gpu: host1x: Allocate gather copy for host1x
- [arm64,armhf] net: dsa: LAN9303: select REGMAP when LAN9303 enable
- [arm64] phy: qcom-usb-hs: Fix extcon double register after power cycle
- [s390x] time: ensure get\_clock\_monotonic() returns monotonic values
- [s390x] mm: add mm\_pxd\_folded() checks to pxd\_free()
- [arm64] net: hns3: add struct netdev\_queue debug info for TX timeout

- libata: Ensure ata\_port probe has completed before detach
- loop: fix no-unmap write-zeroes request behavior
- Bluetooth: Fix advertising duplicated flags
- pinctrl: amd: fix \_\_iomem annotation in amd\_gpio\_irq\_handler()
- ixgbe: protect TX timestamping from API misuse
- media: rcar\_drif: fix a memory disclosure (CVE-2019-18786)
- media: v4l2-core: fix touch support in v4l\_g\_fmt
- rfskill: allocate static minor
- bnx2x: Fix PF-VF communication over multi-cos queues.
- ALSA: timer: Limit max amount of slave instances
- rtlwifi: fix memory leak in rtl92c\_set\_fw\_rsvdpagepkt()
- perf probe: Fix to find range-only function instance
- perf probe: Fix to list probe event with correct line number
- perf jevents: Fix resource leak in process\_mapfile() and main()
- perf probe: Walk function lines in lexical blocks
- perf probe: Fix to probe an inline function which has no entry pc
- perf probe: Fix to show ranges of variables in functions without entry\_pc
- perf probe: Fix to show inlined function callsite without entry\_pc
- perf probe: Fix to probe a function which has no entry pc
- perf tools: Splice events onto evlist even on error
- perf parse: If pmu configuration fails free terms
- perf probe: Skip overlapped location on searching variables
- perf probe: Return a better scope DIE if there is no best scope
- perf probe: Fix to show calling lines of inlined functions
- perf probe: Skip end-of-sequence and non statement lines
- perf probe: Filter out instances except for inlined subroutine and subprogram
- ath10k: fix get invalid tx rate for Mesh metric
- media: pvrusb2: Fix oops on tear-down when radio support is not present
- ice: delay less
- [amd64] spi: pxa2xx: Add missed security checks
- ASoC: rt5677: Mark reg RT5677\_PWR\_ANLG2 as volatile
- iio: dac: ad5446: Add support for new AD5600 DAC
- [x86] ASoC: Intel: kbl\_rt5663\_rt5514\_max98927: Add dmhc format constraint
- [s390x] disassembler: don't hide instruction addresses
- nvme: Discard workaround for non-conformant devices
- parport: load lowlevel driver if ports not found

- bcache: fix static checker warning in `bcache_device_free()`
- cpufreq: Register drivers only after CPU devices have been registered
- tracing: use `kvcalloc` for `tgid_map` array allocation
- tracing/kprobe: Check whether the non-suffixed symbol is `notrace`
- bcache: fix deadlock in `bcache_allocator`
- iwlfwif: mvm: fix unaligned read of `rx_pkt_status`
- [arm64] spi: tegra20-slink: add missed `clk_unprepare`
- tun: fix data-race in `gro_normal_list()`
- crypto: virtio - deal with unsupported input sizes
- btrfs: don't prematurely free work in `end_workqueue_fn()`
- btrfs: don't prematurely free work in `run_ordered_work()`
- [x86] ASoC: Intel: bytcr\_rt5640: Update quirk for Acer Switch 10 SW5-012 2-in-1
- [x86] insn: Add some Intel instructions to the opcode map
- brcmfmac: remove monitor interface when detaching
- iwlfwif: check `kasprintf()` return value
- [armhf] net: ethernet: ti: ale: clean ale tbl on init and intf restart
- [armhf] crypto: sun4i-ss - Fix 64-bit `size_t` warnings
- [armhf] crypto: sun4i-ss - Fix 64-bit `size_t` warnings on `sun4i-ss-hash.c`
- mac80211: consider QoS Null frames for `STA_NULLFUNC_ACKED`
- net: phy: initialise `phydev` speed and duplex sanely
- btrfs: don't prematurely free work in `reada_start_machine_worker()`
- btrfs: don't prematurely free work in `scrub_missing_raid56_worker()`
- Revert "mmc: sdhci: Fix incorrect switch to HS mode"
- can: kvaser\_usb: kvaser\_usb\_leaf: Fix some info-leaks to USB devices (CVE-2019-19947)
- usb: xhci: Fix build warning seen with `CONFIG_PM=n`
- [s390x] ftrace: fix endless recursion in `function_graph` tracer
- btrfs: return error pointer from `alloc_test_extent_buffer`
- usbip: Fix receive error in `vhci-hcd` when using scatter-gather
- usbip: Fix error path of `vhci_recv_ret_submit()`
- cpufreq: Avoid leaving stale IRQ work items during CPU offline
- [x86] intel\_th: pci: Add Comet Lake PCH-V support
- [x86] intel\_th: pci: Add Elkhart Lake SOC support
- [x86] platform/x86: hp-wmi: Make buffer for `HPWMI_FEATURE2_QUERY` 128 bytes
- [x86] staging: comedi: gsc\_hpdi: check `dma_alloc_coherent()` return value
- ext4: fix `ext4_empty_dir()` for directories with holes (CVE-2019-19037)
- ext4: check for directory entries too close to block end

- ext4: unlock on error in ext4\_expand\_extra\_isize()
- [arm64] KVM: Ensure 'params' is initialised when looking up sys register
- [x86] MCE/AMD: Do not use rdmsr\_safe\_on\_cpu() in smca\_configure()
- [x86] MCE/AMD: Allow Reserved types to be overwritten in smca\_banks[]
- [powerpc\*] irq: fix stack overflow verification
- [arm64] mmc: sdhci-msm: Correct the offset and value for DDR\_CONFIG register
- mmc: sdhci: Update the tuning failed messages to pr\_debug level
- mmc: sdhci: Workaround broken command queuing on Intel GLK
- mmc: sdhci: Add a quirk for broken command queuing
- nbd: fix shutdown and recv work deadlock
- perf probe: Fix to show function entry line as probe-able

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.93>

- scsi: lpfc: Fix discovery failures when target device connectivity bounces
- scsi: mpt3sas: Fix clear pending bit in ioctl status
- scsi: lpfc: Fix locking on mailbox command completion
- Input: atmel\_mxt\_ts - disable IRQ across suspend
- f2fs: fix to update time in lazytime mode
- [arm64,armhf] iommu: rockchip: Free domain on .domain\_free
- [arm64,armhf] iommu/tegra-smmu: Fix page tables in > 4 GiB memory
- scsi: target: compare full CHAP\_A Algorithm strings
- scsi: lpfc: Fix SLI3 hba in loop mode not discovering devices
- scsi: csistostor: Don't enable IRQs too early
- [arm64] scsi: hisi\_sas: Replace in\_softirq() check in hisi\_sas\_task\_exec()
- [ppc64el] pseries: Mark accumulate\_stolen\_time() as notrace
- [ppc64el] pseries: Don't fail hash page table insert for bolted mapping
- clocksource/drivers/timer-of: Use unique device name instead of timer
- [ppc64el] security/book3s64: Report L1TF status in sysfs
- [ppc64el] book3s64/hash: Add cond\_resched to avoid soft lockup warning
- ext4: update direct I/O read lock pattern for IOCB\_NOWAIT
- ext4: iomap that extends beyond EOF should be marked dirty
- jbd2: Fix statistics for the number of logged blocks
- scsi: tracing: Fix handling of TRANSFER LENGTH == 0 for READ(6) and WRITE(6)
- scsi: lpfc: Fix duplicate unreg\_rpi error in port offline flow
- f2fs: fix to update dir's i\_pino during cross\_rename
- [arm64] clk: qcom: Allow constant ratio freq tables for rcg
- clk: clk-gpio: propagate rate change to parent

- fs/quota: handle overflows of sysctl fs.quota.\* and report as unsigned long
- scsi: lpfc: fix: Coverity: lpfc\_cmpl\_els\_rsp(): Null pointer dereferences
- [ppc64el] PCI: rpaphp: Fix up pointer to first drc-info entry
- scsi: ufs: fix potential bug which ends in system hang
- [ppc64el] PCI: rpaphp: Don't rely on firmware feature to imply drc-info support
- [ppc64el] PCI: rpaphp: Annotate and correctly byte swap DRC properties
- [ppc64el] PCI: rpaphp: Correctly match ibm, my-drc-index to drc-name when using drc-info
- [ppc64el] powerpc/security: Fix wrong message when RFI Flush is disable
- bcache: at least try to shrink 1 node in bch\_mca\_scan()
- HID: quirks: Add quirk for HP MSU1465 PIXART OEM mouse
- HID: logitech-hidpp: Silence intermittent get\_battery\_capacity errors
- [armhf] 8937/1: spectre-v2: remove Brahma-B53 from hardening
- libnvdimm/btt: fix variable 'rc' set but not used
- HID: Improve Windows Precision Touchpad detection.
- HID: rmi: Check that the RMI\_STARTED bit is set before unregistering the RMI transport device
- watchdog: Fix the race between the release of watchdog\_core\_data and cdev
- scsi: pm80xx: Fix for SATA device discovery
- scsi: ufs: Fix error handing during hibern8 enter
- scsi: scsi\_debug: num\_tgts must be >= 0
- scsi: iscsi: Don't send data to unbound connection
- scsi: target: iscsi: Wait for all commands to finish before freeing a session
- apparmor: fix unsigned len comparison with less than zero
- scripts/kallsyms: fix definitely-lost memory leak
- cdrom: respect device capabilities during opening action
- perf script: Fix brstackinsn for AUXTRACE
- perf regs: Make perf\_reg\_name() return "unknown" instead of NULL
- [s390x] zcrypt: handle new reply code FILTERED\_BY\_HYPERVISOR
- [s390x] cpum\_sf: Check for SDBT and SDB consistency
- ocfs2: fix passing zero to 'PTR\_ERR' warning
- kernel: sysctl: make drop\_caches write-only
- userfaultfd: require CAP\_SYS\_PTRACE for UFFD\_FEATURE\_EVENT\_FORK
- [x86] mce: Fix possibly incorrect severity calculation on AMD
- net, sysctl: Fix compiler warning when only cBPF is present
- netfilter: nf\_queue: enqueue skbs with NULL dst
- ALSA: hda - Downgrade error message for single-cmd fallback
- bonding: fix active-backup transition after link failure

- perf strbuf: Remove redundant va\_end() in strbuf\_adv()
- Make filldir[64]() verify the directory entry filename is valid (CVE-2019-10220)
- filldir[64]: remove WARN\_ON\_ONCE() for bad directory entries (CVE-2019-10220)
- netfilter: ebttables: compat: reject all padding in matches/watchers
- 6pack,mkiss: fix possible deadlock
- netfilter: bridge: make sure to pull arp header in br\_nf\_forward\_arp()
- inetpeer: fix data-race in inet\_putpeer / inet\_putpeer
- net: add a READ\_ONCE() in skb\_peek\_tail()
- net: icmp: fix data-race in cmp\_global\_allow()
- hrtimer: Annotate lockless access to timer->state
- net: ena: fix napi handler misbehavior when the napi budget is zero
- net/mlxfw: Fix out-of-memory error in mfa2 flash burning
- [arm64,armhf] net: stmmac: dwmac-meson8b: Fix the RGMII TX delay on Meson8b/8m2 SoCs
- ptp: fix the race between the release of ptp\_clock and cdev
- tcp: Fix highest\_sack and highest\_sack\_seq
- udp: fix integer overflow while computing available space in sk\_rcvbuf
- vhost/vsock: accept only packets with the right dst\_cid
- net: add bool confirm\_neigh parameter for dst\_ops.update\_pmtu
- ip6\_gre: do not confirm neighbor when do pmtu update
- gtp: do not confirm neighbor when do pmtu update
- net/dst: add new function skb\_dst\_update\_pmtu\_no\_confirm
- tunnel: do not confirm neighbor when do pmtu update
- vti: do not confirm neighbor when do pmtu update
- sit: do not confirm neighbor when do pmtu update
- net/dst: do not confirm neighbor for vxlan and geneve pmtu update
- gtp: do not allow adding duplicate tid and ms\_addr pdp context
- [arm64,armhf] net: marvell: mvpp2: phylink requires the link interrupt
- tcp/dccp: fix possible race \_\_inet\_lookup\_established()
- tcp: do not send empty skb from tcp\_write\_xmit()
- gtp: fix wrong condition in gtp\_genl\_dump\_pdp()
- gtp: fix an use-after-free in ipv4\_pdp\_find()
- gtp: avoid zero size hashtable
- [arm64,armhf] pinctrl: baytrail: Really serialize all register accesses

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.94>

- nvme\_fc: add module to ops template to allow module references
- nvme-fc: fix double-free scenarios on hw queues

- drm/amdgpu: add check before enabling/disabling broadcast mode
- drm/amdgpu: add cache flush workaround to gfx8 emit\_fence
- PM / devfreq: Fix devfreq\_notifier\_call returning errno
- PM / devfreq: Set scaling\_max\_freq to max on OPP notifier error
- PM / devfreq: Don't fail devfreq\_dev\_release if not in list
- afs: Fix afs\_find\_server lookups for ipv4 peers
- afs: Fix SELinux setting security label on /afs
- RDMA/cma: add missed unregister\_pernet\_subsys in init failure
- rxe: correctly calculate iCRC for unaligned payloads
- scsi: lpfc: Fix memory leak on lpfc\_bsg\_write\_ebuf\_set func
- scsi: qla2xxx: Drop superfluous INIT\_WORK of del\_work
- scsi: qla2xxx: Don't call qlt\_async\_event twice
- scsi: qla2xxx: Fix PLOGI payload and ELS IOCB dump length
- scsi: qla2xxx: Configure local loop for N2N target
- scsi: qla2xxx: Send Notify ACK after N2N PLOGI
- scsi: qla2xxx: Ignore PORT UPDATE after N2N PLOGI
- scsi: iscsi: qla4xxx: fix double free in probe
- scsi: libsas: stop discovering if oob mode is disconnected (CVE-2019-19965)
- drm/nouveau: Move the declaration of struct nouveau\_conn\_atom up a bit
- usb: gadget: fix wrong endpoint desc
- net: make socket read/write\_iter() honor IOCB\_NOWAIT
- afs: Fix creation calls in the dynamic root to fail with EOPNOTSUPP
- md: raid1: check rdev before reference in raid1\_sync\_request func
- [s390x] cpum\_sf: Adjust sampling interval to avoid hitting sample limits
- [s390x] cpum\_sf: Avoid SBD overflow condition in irq handler
- IB/mlx4: Follow mirror sequence of device add during device removal
- IB/mlx5: Fix steering rule of drop and count
- xen-blkback: prevent premature module unload
- xen/balloon: fix ballooned page accounting without hotplug enabled
- PM / hibernate: memory\_bm\_find\_bit(): Tighten node optimisation
- ALSA: hda/realtek - Add Bass Speaker and fixed dac for bass speaker
- ALSA: hda/realtek - Enable the bass speaker of ASUS UX431FLC
- ALSA: hda - fixup for the bass speaker on Lenovo Carbon X1 7th gen
- xfs: fix mount failure crash on invalid iclog memory access
- taskstats: fix data-race
- drm: limit to INT\_MAX in create\_blob ioctl



- netfilter: nft\_tproxy: Fix port selector on Big Endian
- ALSA: ice1724: Fix sleep-in-atomic in Infrasonic Quartet support code
- ALSA: usb-audio: fix set\_format altsetting sanity check
- ALSA: usb-audio: set the interface format after resume on Dell WD19
- ALSA: hda/realtek - Add headset Mic no shutup for ALC283
- [arm64,armhf] drm/sun4i: hdmi: Remove duplicate cleanup calls
- [mips\*] Avoid VDSO ABI breakage due to global register variable
- media: pulse8-cec: fix lost cec\_transmit\_attempt\_done() call
- media: cec: CEC 2.0-only bcast messages were ignored
- media: cec: avoid decrementing transmit\_queue\_sz if it is 0
- media: cec: check 'transmit\_in\_progress', not 'transmitting'
- mm/zsmalloc.c: fix the migrated zspage statistics.
- memcg: account security cred as well to kmemcg
- mm: move\_pages: return valid node id in status if the page is already on the target node
- [x86,arm64] pstore/ram: Write new dumps to start of recycled zones
- locks: print unsigned ino in /proc/locks
- compat\_ioctl: block: handle Persistent Reservations
- compat\_ioctl: block: handle BLKREPORTZONE/BLKRESETZONE
- ata: libahci\_platform: Export again ahci\_platform\_<en/dis>able\_phys()
- libata: Fix retrieving of active qcs
- gpiolib: fix up emulated open drain outputs
- tracing: Fix lock inversion in trace\_event\_enable\_tgid\_record()
- tracing: Avoid memory leak in process\_system\_preds()
- tracing: Have the histogram compare functions convert to u64 first
- tracing: Fix endianness bug in histogram trigger
- apparmor: fix aa\_xattrs\_match() may sleep while holding a RCU lock
- [i386] ALSA: cs4236: fix error return comparison of an unsigned integer
- ALSA: firewire-motu: Correct a typo in the clock proc string
- exit: panic before exit\_mm() on global init exit
- [arm64] Revert support for execute-only user mappings
- ftrace: Avoid potential division by zero in function profiler
- [arm64] drm/msm: include linux/sched/task.h
- PM / devfreq: Check NULL governor in available\_governors\_show
- nfsd4: fix up replay\_matches\_cache()
- [x86,arm64] HID: i2c-hid: Reset ALPS touchpads on resume
- ACPI: sysfs: Change ACPI\_MASKABLE\_GPE\_MAX to 0x100

- xfs: don't check for AG deadlock for realtime files in bunmap
- [x86] platform/x86: pmc\_atom: Add Siemens CONNECT X300 to critclk\_systems DMI table
- Bluetooth: btusb: fix PM leak in error case of setup
- Bluetooth: delete a stray unlock
- Bluetooth: Fix memory leak in hci\_connect\_le\_scan
- media: flexcop-usb: ensure -EIO is returned on error condition
- media: usb: fix memory leak in af9005\_identify\_state (CVE-2019-18809)
- [arm64] dts: meson: odroid-c2: Disable usb\_otg bus to avoid power failed warning
- [arm64] tty: serial: msm\_serial: Fix lockup for sysrq and oops
- fix compat handling of FICLONERANGE, FIDEDUPERANGE and FS\_IOC\_FIEMAP
- bdev: Factor out bdev revalidation into a common helper
- bdev: Refresh bdev size for disks without partitioning
- scsi: qedf: Do not retry ELS request if qedf\_alloc\_cmd fails
- drm/mst: Fix MST sideband up-reply failure handling
- [ppc64el] pseries/hvconsole: Fix stack overread via udbg
- [ppc64el] KVM: PPC: Book3S HV: use smp\_mb() when setting/clearing host\_ipi flag
- rxrpc: Fix possible NULL pointer access in ICMP handling
- tcp: annotate tp->rcv\_nxt lockless reads
- net: core: limit nested device depth
- ath9k\_htc: Modify byte order for an error message
- ath9k\_htc: Discard undersized packets
- xfs: periodically yield scrub threads to the scheduler
- net: add annotations on hh->hh\_len lockless accesses
- ubifs: ubifs\_tnc\_start\_commit: Fix OOB in layout\_in\_gaps
- [s390x] smp: fix physical to logical CPU map for SMT
- xen/blkback: Avoid unmapping unmapped grant pages
- [x86] perf/x86/intel/bts: Fix the use of page\_private()

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.95>

- bpf: Fix passing modified ctx to ld/abs/ind instruction
- regulator: fix use after free issue
- ASoC: max98090: fix possible race conditions
- netfilter: ctnetlink: netns exit must wait for callbacks
- mwifiex: Fix heap overflow in mmwifiex\_process\_tdl\_action\_frame() (CVE-2019-14901)
- [x86] efi: Update e820 with reserved EFI boot services data to fix kexec breakage
- [x86] ASoC: Intel: bytcr\_rt5640: Update quirk for Teclast X89
- efi/gop: Return EFI\_NOT\_FOUND if there are no usable GOPs

- efi/gop: Return EFI\_SUCCESS if a usable GOP was found
- efi/gop: Fix memory leak in \_\_gop\_query32/64()
- netfilter: uapi: Avoid undefined left-shift in xt\_sctp.h
- netfilter: nft\_set\_rbtrees: bogus lookup/get on consecutive elements in named sets
- netfilter: nf\_tables: validate NFT\_SET\_ELEM\_INTERVAL\_END
- netfilter: nf\_tables: validate NFT\_DATA\_VALUE after nft\_data\_init()
- [arm64] spi: spi-cavium-thunderx: Add missing pci\_release\_regions()
- ASoC: topology: Check return value for soc\_tplg\_pcm\_create()
- bnx2\_en: Return error if FW returns more data than dump length
- [mips\*] bpf, mips: Limit to 33 tail calls
- [armhf] spi: spi-ti-qspi: Fix a bug when accessing non default CS
- [powerpc\*] Ensure that swiotlb buffer is allocated from low memory
- btrfs: Fix error messages in qgroup\_rescan\_init
- bpf: Clear skb->tstamp in bpf\_redirect when necessary
- bnx2x: Do not handle requests from VFs after parity
- bnx2x: Fix logic to get total no. of PFs per engine
- cxgb4: Fix kernel panic while accessing sge\_info
- net: usb: lan78xx: Fix error message format specifier
- rfskill: Fix incorrect check to avoid NULL pointer dereference
- iommu/iova: Init the struct iova to fix the possible memleak
- [x86] perf/x86/intel: Fix PT PMI handling
- fs: avoid softlockups in s\_inodes iterators
- [arm64,armhf] net: stmmac: Do not accept invalid MTU values
- [arm64,armhf] net: stmmac: xgmac: Clear previous RX buffer size
- [arm64,armhf] net: stmmac: RX buffer size must be 16 byte aligned
- [arm64,armhf] net: stmmac: Always arm TX Timer at end of transmission start
- [s390x] dasd/cio: Interpret ccw\_device\_get\_mdc return value correctly
- [s390x] dasd: fix memleak in path handling error case
- block: fix memleak when \_\_blk\_rq\_map\_user\_iov() is failed
- llc2: Fix return statement of llc\_stat\_ev\_rx\_null\_dsap\_xid\_c (and \_test\_c)
- [x86] hv\_netvsc: Fix unwanted rx\_table reset
- [powerpc\*] vcpu: Assume dedicated processors as non-preempt
- [powerpc\*] spinlocks: Include correct header for static key
- [armhf] cpufreq: imx6q: read OCOTP through nvmmem for imx6ul/imx6ull
- gtp: fix bad unlock balance in gtp\_encap\_enable\_socket
- macvlan: do not assume mac\_header is set in macvlan\_broadcast()

- [arm64,armhf] net: dsa: mv88e6xxx: Preserve priority when setting CPU port.
- [arm64,armhf] net: stmmac: dwmac-sun8i: Allow all RGMII modes
- [arm64,armhf] net: stmmac: dwmac-sunxi: Allow all RGMII modes
- net: usb: lan78xx: fix possible skb leak
- pkt\_sched: fq: do not accept silly TCA\_FQ\_QUANTUM
- sch\_cake: avoid possible divide by zero in cake\_enqueue()
- sctp: free cmd->obj.chunk for the unprocessed SCTP\_CMD\_REPLY
- tcp: fix "old stuff" D-SACK causing SACK to be treated as D-SACK
- vxlan: fix tos value before xmit
- vlan: fix memory leak in vlan\_dev\_set\_egress\_priority
- vlan: vlan\_changelink() should propagate errors
- net: sch\_prio: When ungrafting, replace with FIFO
- [arm64,armhf] usb: dwc3: gadget: Fix request complete check
- USB: core: fix check for duplicate endpoints
- USB: serial: option: add Telit ME910G1 0x110a composition
- usb: missing parentheses in USE\_NEW\_SCHEME

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.96>

- chardev: Avoid potential use-after-free in 'chrdev\_open()'
- i2c: fix bus recovery stop mode timing
- [arm64,armhf] usb: chipidea: host: Disable port power only if previously enabled
- ALSA: usb-audio: Apply the sample rate quirk for Bose Companion 5
- ALSA: hda/realtek - Add new codec supported for ALCS1200A
- ALSA: hda/realtek - Set EAPD control to default for ALC222
- [x86] ALSA: hda/realtek - Add quirk for the bass speaker on Lenovo Yoga X1 7th gen
- kernel/trace: Fix do not unregister tracepoints when register sched\_migrate\_task fail
- tracing: Have stack tracer compile when MCOUNT\_INSN\_SIZE is not defined
- tracing: Change offset type to s32 in preempt/irq tracepoints
- HID: Fix slab-out-of-bounds read in hid\_field\_extract
- HID: uhid: Fix returning EPOLLOUT from uhid\_char\_poll
- HID: hid-input: clear unmapped usages
- Input: add safety guards to input\_set\_keycode()
- [arm64,armhf] drm/sun4i: tcon: Set RGB DCLK min. divider based on hardware model
- drm/fb-helper: Round up bits\_per\_pixel if possible
- drm/dp\_mst: correct the shifting in DP\_REMOTE\_I2C\_READ
- can: kvaser\_usb: fix interface sanity check
- can: gs\_usb: gs\_usb\_probe(): use descriptors of current altsetting

- can: can\_dropped\_invalid\_skb(): ensure an initialized headroom in outgoing CAN sk\_buffs
- gpiolib: acpi: Turn dmi\_system\_id table into a generic quirk table
- gpiolib: acpi: Add honor\_wakeup module-option + quirk mechanism
- [x86] staging: vt6656: set usb\_set\_intfdata on driver fail.
- USB: serial: option: add ZLP support for 0x1bc7/0x9010
- [arm64,armhf] usb: musb: fix idling for suspend after disconnect interrupt
- [arm64,armhf] usb: musb: Disable pullup at init
- [arm64,armhf] usb: musb: dma: Correct parameter passed to IRQ handler
- [x86] staging: comedi: adv\_pci1710: fix AI channels 16-31 for PCI-1713
- staging: rtl8188eu: Add device code for TP-Link TL-WN727N v5.21
- serdev: Don't claim unsupported ACPI serial devices
- tty: link tty and port before configuring it as console
- tty: always relink the port
- mwifiex: fix possible heap overflow in mwifiex\_process\_country\_ie() (CVE-2019-14895)
- mwifiex: pcie: Fix memory leak in mwifiex\_pcie\_alloc\_cmdrsp\_buf (CVE-2019-19056)
- scsi: bfa: release allocated memory in case of error (CVE-2019-19066)
- rtl8xxxu: prevent leaking urb (CVE-2019-19068)
- ath10k: fix memory leak (CVE-2019-19078)
- HID: hiddev: fix mess in hiddev\_open()
- USB: Fix: Don't skip endpoint descriptors with maxpacket=0
- netfilter: arp\_tables: init netns pointer in xt\_tgchk\_param struct
- netfilter: conntrack: dccp, sctp: handle null timeout argument
- netfilter: ipset: avoid null deref when IPSET\_ATTR\_LINENO is present
- [x86] drm/i915/gen9: Clear residual context state on context switch (CVE-2019-14615)

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.97>

- hidraw: Return EPOLLOUT from hidraw\_poll
- HID: hidraw: Fix returning EPOLLOUT from hidraw\_poll
- HID: hidraw, uhid: Always report EPOLLOUT
- cfg80211/mac80211: make ieee80211\_send\_layer2\_update a public function
- mac80211: Do not send Layer 2 Update frame before authorization (CVE-2019-5108)
- f2fs: Move err variable to function scope in f2fs\_fill\_dentries()
- f2fs: check memory boundary by insane namelen
- f2fs: check if file namelen exceeds max value (CVE-2019-9445)
- media: usb: zr364xx: Fix KASAN: null-ptr-deref Read in zr364xx\_vidioc\_querycap (CVE-2019-15217)
- iwlmwifi: dbg\_ini: fix memory leak in alloc\_shtable (CVE-2019-19058)
- iwlmwifi: pcie: fix memory leaks in iwl\_pcie\_ctxt\_info\_gen3\_init (CVE-2019-19059)

- RDMA: Fix goto target to release the allocated memory (CVE-2019-19077)
- dccp: Fix memleak in \_\_feat\_register\_sp (CVE-2019-20096)
- [x86] drm/i915: Fix use-after-free when destroying GEM context
- ASoC: soc-core: Set dpcm\_playback / dpcm\_capture
- [armhf] mtd: onenand: omap2: Pass correct flags for prep\_dma\_memcpy
- [arm64] gpio: zynq: Fix for bug in zynq\_gpio\_restore\_context API
- iommu: Remove device link to group on failure
- gpio: Fix error message on out-of-range GPIO in lookup table
- [s390x] qeth: fix false reporting of VNIC CHAR config failure
- [s390x] qeth: Fix vnice\_is\_in\_use if rx\_bcast not set
- cifs: Adjust indentation in smb2\_open\_file
- afs: Fix missing cell comparison in afs\_test\_super()
- drm/ttm: fix start page for huge page check in ttm\_put\_pages() (CVE-2019-19927)
- drm/ttm: fix incrementing the page pointer for huge pages (CVE-2019-19927)
- btrfs: simplify inode locking for RWF\_NOWAIT
- RDMA/mlx5: Return proper error value
- RDMA/srpt: Report the SCSI residual to the initiator
- scsi: enclosure: Fix stale device oops with hot replug
- scsi: sd: Clear sdkp->protection\_type if disk is reformatted without PI
- [x86] platform/x86: asus-wmi: Fix keyboard brightness cannot be set to 0
- [x86] platform/x86: GPD pocket fan: Use default values when wrong modparams are given
- xprtrdma: Fix completion wait during device removal
- crypto: virtio - implement missing support for output IVs
- NFSv2: Fix a typo in encode\_sattr()
- NFSv4.x: Drop the slot if nfs4\_delegreturn\_prepare waits for layoutreturn
- mei: fix modalias documentation
- [armhf] clk: samsung: exynos5420: Preserve CPU clocks configuration during suspend/resume
- [armhf] pinctl: ti: iodelay: fix error checking on pinctrl\_count\_index\_with\_args call
- [x86] pinctrl: lewisburg: Update pin list according to v1.1v6
- scsi: sd: enable compat ioctls for sed-opal
- af\_unix: add compat\_ioctl support
- compat\_ioctl: handle SIOCOUTQNSD
- [arm64,armhf] PCI: dwc: Fix find\_next\_bit() usage
- PCI/PTM: Remove spurious "d" from granularity message
- [powerpc\*] powernv: Disable native PCIe port management
- [armhf] tty: serial: imx: use the sg count from dma\_map\_sg

- [i386] tty: serial: pch\_uart: correct usage of dma\_unmap\_sg
- mtd: spi-nor: fix silent truncation in spi\_nor\_read()
- mtd: spi-nor: fix silent truncation in spi\_nor\_read\_raw()
- rtlwifi: Remove unnecessary NULL check in rtl\_regd\_init
- f2fs: fix potential overflow
- scsi: libcxgbi: fix NULL pointer dereference in cxgbi\_device\_destroy()
- [mips\*] cacheinfo: report shared CPU map
- [arm64] drm/arm/mali: make malidp\_mw\_connector\_helper\_funcs static
- [arm64] dmaengine: k3dma: Avoid null pointer traversal
- [amd64] ioat: ioat\_alloc\_ring() failure handling.
- ocfs2: call journal flush to mark journal as empty after journal recovery when mount

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.98>

- clk: Don't try to enable critical clocks if prepare failed
- iio: buffer: align the size of scan bytes to size of the largest element
- USB: serial: simple: Add Motorola Solutions TETRA MTP3xxx and MTP85xx
- USB: serial: option: Add support for Quectel RM500Q
- USB: serial: opticon: fix control-message timeouts
- USB: serial: option: add support for Quectel RM500Q in QDL mode
- USB: serial: suppress driver bind attributes
- USB: serial: ch341: handle unbound port at reset\_resume
- USB: serial: io\_edgeport: handle unbound ports on URB completion
- USB: serial: io\_edgeport: add missing active-port sanity check
- USB: serial: keyspan: handle unbound ports
- USB: serial: quatech2: handle unbound ports
- [x86] scsi: fnic: fix invalid stack access
- scsi: mptfusion: Fix double fetch bug in ioctl
- [armhf] dts: imx6q-dhcom: Fix SGTL5000 VDDIO regulator connection
- ALSA: dice: fix fallback from protocol extension into limited functionality
- ALSA: seq: Fix racy access for queue timer in proc read
- ALSA: usb-audio: fix sync-ep altsetting sanity check
- [arm64] dts: allwinner: a64: olinuxino: Fix SDIO supply regulator
- block: fix an integer overflow in logical block size
- [armhf] dts: am571x-idk: Fix gpios property to have the correct gpio number
- LSM: generalize flag passing to security\_capable
- ptrace: reintroduce usage of subjective credentials in ptrace\_has\_cap()
- usb: core: hub: Improved device recognition on remote wakeup

- [x86] resctrl: Fix an imbalance in domain\_remove\_cpu()
- [x86] CPU/AMD: Ensure clearing of SME/SEV features is maintained
- [amd64] x86/efistub: Disable paging at mixed mode entry
- [x86] resctrl: Fix potential memory leak
- perf histograms: Fix variable name's inconsistency in histograms\_for\_each() macro
- perf report: Fix incorrectly added dimensions as switch perf data file
- mm/shmem.c: thp, shmem: fix conflict of above-47bit hint address and PMD alignment
- mm: memcg/slab: call flush\_memcg\_workqueue() only if memcg workqueue is valid
- btrfs: rework arguments of btrfs\_unlink\_subvol
- btrfs: fix invalid removal of root ref
- btrfs: do not delete mismatched root refs
- btrfs: fix memory leak in qgroup accounting
- mm/page-writeback.c: avoid potential division by zero in wb\_min\_max\_ratio()
- [armhf] dts: imx6qdl: Add Engicam i.Core 1.5 MX6
- [armhf] dts: imx6q-icore-mipi: Use 1.5 version of i.Core MX6DL
- [arm64,armhf] net: stmmac: 16KB buffer must be 16 byte aligned
- [arm64,armhf] net: stmmac: Enable 16KB buffer size
- mm/huge\_memory.c: make \_\_thp\_get\_unmapped\_area static
- mm/huge\_memory.c: thp: fix conflict of above-47bit hint address and PMD alignment
- bpf: Fix incorrect verifier simulation of ARSH under ALU32
- cfg80211: fix deadlocks in autodisconnect work
- cfg80211: fix memory leak in cfg80211\_cqm\_rssi\_update
- cfg80211: fix page refcount issue in A-MSDU decap
- netfilter: fix a use-after-free in mtype\_destroy()
- netfilter: arp\_tables: init netns pointer in xt\_tgdtor\_param struct
- netfilter: nft\_tunnel: fix null-attribute check
- netfilter: nf\_tables: remove WARN and add NLA\_STRING upper limits
- netfilter: nf\_tables: store transaction list locally while requesting module
- netfilter: nf\_tables: fix flowtable list del corruption
- NFC: pn533: fix bulk-message timeout
- batman-adv: Fix DAT candidate selection on little endian systems
- macvlan: use skb\_reset\_mac\_header() in macvlan\_queue\_xmit()
- [x86] hv\_netvsc: Fix memory leak when removing rndis device
- [arm64] net: hns: fix soft lockup when there is not enough memory
- net: usb: lan78xx: limit size of local TSO packets
- ptp: free ptp device pin descriptors properly



- r8152: add missing endpoint sanity check
- tcp: fix marked lost packets not being retransmitted
- xen/blkfront: Adjust indentation in xlvbd\_alloc\_gendisk
- tcp: refine rule to allow EPOLLOUT generation under mem pressure
- [arm64] dts: meson-gxl-s905x-khadas-vim: fix gpio-keys-pollled node
- cfg80211: check for set\_wiphy\_params
- tick/sched: Annotate lockless access to last\_jiffies\_update
- drm/nouveau/bar/nv50: check bar1 vmm return value
- drm/nouveau/bar/gf100: ensure BAR is mapped
- drm/nouveau/mmu: qualify vmm during dtor
- reiserfs: fix handling of -EOPNOTSUPP in reiserfs\_for\_each\_xattr
- scsi: esas2r: unlock on error in esas2r\_nvram\_read\_direct()
- scsi: qla4xxx: fix double free bug
- scsi: bnx2i: fix potential use after free
- scsi: target: core: Fix a pr\_debug() argument
- scsi: qla2xxx: Fix qla2x00\_request\_irqs() for MSI
- scsi: qla2xxx: fix rports not being mark as lost in sync fabric scan
- scsi: core: scsi\_trace: Use get\_unaligned\_be\*()
- perf probe: Fix wrong address verification

Joe Richey

- [cloud-amd64] tpm: Enable TPM drivers for Cloud (Closes: #946237)

Salvatore Bonaccorso

- Refresh powerpc-fix-mcpu-options-for-spe-only-compiler.patch (Context changes in 4.19.88)
- Drop 0027-RDMA-hns-Fix-the-bug-with-updating-rq-head-pointer-w.patch
- Drop 0028-RDMA-hns-Bugfix-for-the-scene-without-receiver-queue.patch
- [rt] Refresh 0199-net-move-xmit\_recursion-to-per-task-variable-on-RT.patch (Context changes in 4.19.88)
- [rt] Update to 4.19.90-rt35:
  - Update “workqueue: rework” for workqueue changes in 4.19.90
- [rt] Drop 0245-Revert-arm64-preempt-Fix-big-endian-when-checking-pr.patch
- Refresh 0013-scsi-hisi\_sas-Relocate-some-codes-to-avoid-an-unused.patch for context changes in 4.19.93.
- [rt] Refresh 0253-watchdog-prevent-deferral-of-watchdogd-wakeup-on-RT.patch (Context changes in 4.19.93)
- [rt] Refresh 0199-net-move-xmit\_recursion-to-per-task-variable-on-RT.patch (Context changes in 4.19.97)

Ben Hutchings

- [rt] Update to 4.19.94-rt38:
  - Refresh “x86/ioapic: Don’t let setaffinity unmask threaded EOI interrupt too early” which was partly included in 4.19.92

- aufs: Update support patchset to aufs4.19.63+ 20200113; no functional changes
- Bump ABI to 8
- libertas: Fix two buffer overflows at parsing bss descriptor (CVE-2019-14896, CVE-2019-14897)
- wimax: i2400: fix memory leak (CVE-2019-19051)
- wimax: i2400: Fix memory leak in i2400m\_op\_rfkill\_sw\_toggle (CVE-2019-19051)
- [amd64/cloud-amd64] hwrandom: Enable HW\_RANDOM\_VIRTIO (Closes: #914511)

Noah Meyerhans

- random: try to actively add entropy rather than passively wait for it (Closes: #948519)

Aurelien Jarno

- [mips\*/malta] Enable POWER\_RESET\_PIIX4\_POWEROFF.

### 3.14.2 4.19.87-1 - 03. December 2019

- New upstream stable update: <https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.68>
  - seq\_file: fix problem when seeking mid-record
  - mm/hmm: fix bad subpage pointer in try\_to\_unmap\_one
  - mm: mempolicy: make the behavior consistent when MPOL\_MF\_MOVE\* and MPOL\_MF\_STRICT were specified
  - mm: mempolicy: handle vma with unmovable pages mapped correctly in mbind
  - mm/memcontrol.c: fix use after free in mem\_cgroup\_iter()
  - mm/usercopy: use memory range to be accessed for wraparound check
  - Revert “pwm: Set class for exported channels in sysfs”
  - cpufreq: schedutil: Don’t skip freq update when limits change
  - [x86] ALSA: hda/realtek - Add quirk for HP Envy x360
  - ALSA: hda - Apply workaround for another AMD chip 1022:1487
  - ALSA: hda - Fix a memory leak bug
  - ALSA: hda - Add a generic reboot\_notify
  - ALSA: hda - Let all conexant codec enter D3 when rebooting
  - HID: holtek: test for sanity of intfdata
  - HID: hiddev: avoid opening a disconnected device
  - HID: hiddev: do cleanup in failure of opening a device
  - Input: kbtabs - sanity check for endpoint type
  - Input: iforce - add sanity checks
  - net: usb: pegasus: fix improper read if get\_registers() fail
  - netfilter: ebtabs: also count base chain policies
  - xen/pciback: remove set but not used variable ‘old\_state’
  - [armhf,arm64] irqchip/gic-v3-its: Free unused vpt\_page when alloc vpe table fail

- perf header: Fix divide by zero error if f\_header.attr\_size==0
- perf header: Fix use of uninitialized value warning
- libata: zpodd: Fix small read overflow in zpodd\_get\_mech\_type()
- Btrfs: fix deadlock between fiemap and transaction commits
- scsi: hpsa: correct scsi command status issue after reset
- scsi: qla2xxx: Fix possible fcpport null-pointer dereferences
- drm/amdgpu: fix a potential information leaking bug
- ata: libahci: do not complain in case of deferred probe
- kbuild: modpost: handle KBUILD\_EXTRA\_SYMBOLS only for external modules
- [arm64] efi: fix variable 'si' set but not used
- [arm64] unwind: Prohibit probing on return\_address()
- [arm64] mm: fix variable 'pud' set but not used
- IB/core: Add mitigation for Spectre V1
- IB/mlx5: Fix MR registration flow to use UMR properly
- IB/mad: Fix use-after-free in ib mad completion handling
- [arm64] drm: msm: Fix add\_gpu\_components
- [armhf] drm/exynos: fix missing decrement of retry counter
- ocfs2: remove set but not used variable 'last\_hash'
- asm-generic: fix -Wtype-limits compiler warnings
- [arm64] KVM: regmap: Fix unexpected switch fall-through
- [armhf,arm64] KVM: Sync ICH\_VMCR\_EL2 back when about to block
- [x86] staging: comedi: dt3000: Fix signed integer overflow 'divider \* base'
- [x86] staging: comedi: dt3000: Fix rounding up of timer divisor
- USB: core: Fix races in character device registration and deregistraion
- usb: cdc-acm: make sure a refcount is taken early enough
- USB: CDC: fix sanity checks in CDC union parser
- USB: serial: option: add D-Link DWM-222 device ID
- USB: serial: option: Add support for ZTE MF871A
- USB: serial: option: add the BroadMobi BM818 card
- USB: serial: option: Add Motorola modem UARTs
- [x86] drm/i915/cfl: Add a new CFL PCI ID.
- [arm64] ftrace: Ensure module ftrace trampoline is coherent with I-side
- Input: psmouse - fix build error of multiple definition
- bnx2x: Fix VF's VLAN reconfiguration in reload.
- bonding: Add vlan tx offload to hw\_enc\_features
- net: dsa: Check existence of .port\_mdb\_add callback before calling it

- net/mlx4\_en: fix a memory leak bug
- net/packet: fix race in tpacket\_snd()
- sctp: fix memleak in sctp\_send\_reset\_streams
- sctp: fix the transport error\_count check
- team: Add vlan tx offload to hw\_enc\_features
- tipc: initialise addr\_trail\_end when setting node addresses
- xen/netback: Reset nr\_frags before freeing skb
- net/mlx5e: Only support tx/rx pause setting for port owner
- net/mlx5e: Use flow keys dissector to parse packets for ARFS
- [arm64] mmc: sdhci-of-arasan: Do now show error message in case of deferred probe

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.69>

- HID: Add 044f:b320 ThrustMaster, Inc. 2 in 1 DT
- [mips\*] kernel: only use i8253 clocksource with periodic clockevent
- [mips\*] fix cacheinfo
- netfilter: ebttables: fix a memory leak bug in compat
- ASoC: dapm: Fix handling of custom\_stop\_condition on DAPM graph walks
- bonding: Force slave speed check after link state recovery for 802.3ad
- [armhf,arm64] net: mvpp2: Don't check for 3 consecutive Idle frames for 10G links
- can: dev: call netif\_carrier\_off() in register\_candev()
- can: gw: Fix error path of cgw\_module\_init
- [armhf,arm64] ASoC: rockchip: Fix mono capture
- [armhf] ASoC: ti: davinci-mcasp: Correct slot\_width posed constraint
- net: usb: qmi\_wwan: Add the BroadMobi BM818 card
- qed: RDMA - Fix the hw\_ver returned in device attributes
- isdn: mISDN: hfcsusb: Fix possible null-pointer dereferences in start\_isoc\_chain()
- mac80211\_hwsim: Fix possible null-pointer dereferences in hwsim\_dump\_radio\_nl()
- netfilter: ipset: Actually allow destination MAC address for hash:ip,mac sets too
- netfilter: ipset: Copy the right MAC address in bitmap:ip,mac and hash:ip,mac sets
- netfilter: ipset: Fix rename concurrency with listing
- rxrpc: Fix potential deadlock
- rxrpc: Fix the lack of notification when sendmsg() fails on a DATA packet
- isdn: hfcsusb: Fix mISDN driver crash caused by transfer buffer on the stack
- net: phy: phy\_led\_triggers: Fix a possible null-pointer dereference in phy\_led\_trigger\_change\_speed()
- can: sjal000: force the string buffer NULL-terminated
- can: peak\_usb: force the string buffer NULL-terminated
- net/ethernet/qlogic/qed: force the string buffer NULL-terminated

- NFSv4: Fix a potential sleep while atomic in nfs4\_do\_reclaim()
- NFS: Fix regression whereby fscache errors are appearing on 'nofsc' mounts
- HID: quirks: Set the INCREMENT\_USAGE\_ON\_DUPLICATE quirk on Saitek X52
- HID: input: fix a4tech horizontal wheel custom usage
- [armhf,arm64] drm/rockchip: Suspend DP late
- SMB3: Fix potential memory leak when processing compound chain
- SMB3: Kernel oops mounting an encryptData share with CONFIG\_DEBUG\_VIRTUAL
- [s390x] put \_stext and \_etext into .text section
- net: cxgb3\_main: Fix a resource leak in an error path in 'init\_one()'
- [armhf,arm64] net: stmmac: Fix issues when number of Queues >= 4
- [armhf,arm64] net: stmmac: tc: Do not return a fragment entry
- [arm64] net: hisilicon: make hip04\_tx\_reclaim non-reentrant
- [arm64] net: hisilicon: fix hip04-xmit never return TX\_BUSY
- [arm64] net: hisilicon: Fix dma\_map\_single failed on arm64
- libata: have ata\_scsi\_rw\_xlat() fail invalid passthrough requests
- libata: add SG safety checks in SFF pio transfers
- [x86] lib/cpu: Address missing prototypes warning
- [x86] drm/vmwgfx: fix memory leak when too many retries have occurred
- block, bfq: handle NULL return value by bfq\_init\_rq()
- perf ftrace: Fix failure to set cpumask when only one cpu is present
- perf cpumap: Fix writing to illegal memory in handling cpumap mask
- perf pmu-events: Fix missing "cpu\_clk\_unhalted.core" event
- [arm64] KVM: Don't write junk to sysregs on reset
- [armhf] KVM: Don't write junk to CP15 registers on reset
- HID: wacom: correct misreported EKR ring values
- HID: wacom: Correct distance scale for 2nd-gen Intuos devices
- Revert "dm bufio: fix deadlock with loop device" (regression in 4.19.61)
- ceph: clear page dirty before invalidate page
- ceph: don't try fill file\_lock on unsuccessful GETFILELOCK reply
- libceph: fix PG split vs OSD (re)connect race
- drm/nouveau: Don't retry infinitely when receiving no data on i2c over AUX
- gpiolib: never report open-drain/source lines as 'input' to user-space
- [x86] Drivers: hv: vmbus: Fix virt\_to\_hvfn() for X86\_PAE
- userfaultfd\_release: always remove uffd flags and clear vm\_userfaultfd\_ctx
- [i386] retpoline: Don't clobber RFLAGS during CALL\_NOSPEC on i386
- [x86] apic: Handle missing global clockevent gracefully

- [x86] CPU/AMD: Clear RDRAND CPUID bit on AMD family 15h/16h
- [x86] boot: Save fields explicitly, zero out everything else
- [x86] boot: Fix boot regression caused by bootparam sanitizing
- dm kcopyd: always complete failed jobs
- dm btree: fix order of block initialization in btree\_split\_beneath
- dm integrity: fix a crash due to BUG\_ON in \_\_journal\_read\_write()
- dm raid: add missing cleanup in raid\_ctr()
- dm space map metadata: fix missing store of apply\_bops() return value
- dm table: fix invalid memory accesses with too high sector number
- dm zoned: improve error handling in reclaim
- dm zoned: improve error handling in i/o map code
- dm zoned: properly handle backing device failure
- genirq: Properly pair kobject\_del() with kobject\_add()
- mm, page\_owner: handle THP splits correctly
- mm/zsmalloc.c: migration can leave pages in ZS\_EMPTY indefinitely
- mm/zsmalloc.c: fix race condition in zs\_destroy\_pool
- xfs: don't trip over uninitialized buffer on extent read of corrupted inode
- xfs: Move fs/xfs/xfs\_attr.h to fs/xfs/libxfs/xfs\_attr.h
- xfs: Add helper function xfs\_attr\_try\_sf\_addname
- xfs: Add attribute set and helper functions
- xfs: Add attribute remove and helper functions
- xfs: always rejoin held resources during defer roll
- dm zoned: fix potential NULL dereference in dmz\_do\_reclaim()
- [ppc64el] Allow flush\_(invalid\_)dcache\_range to work across ranges >4GB
- rxrpc: Fix local endpoint refcounting
- rxrpc: Fix read-after-free in rxrpc\_queue\_local()
- rxrpc: Fix local endpoint replacement
- rxrpc: Fix local refcounting

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.70>

- nvme-multipath: revalidate nvme\_ns\_head gendisk in nvme\_validate\_ns
- afs: Fix the CB.ProbeUuid service handler to reply correctly
- afs: Fix loop index mixup in afs\_deliver\_vl\_get\_entry\_by\_name\_u()
- fs: afs: Fix a possible null-pointer dereference in afs\_put\_read()
- afs: Only update d\_fsdata if different in afs\_d\_revalidate()
- nvmet-loop: Flush nvme\_delete\_wq when removing the port
- nvme: fix a possible deadlock when passthru commands sent to a multipath device

- nvme-pci: Fix async probe remove race
- [armhf] omap-dma/omap\_vout\_vrfb: fix off-by-one fi value
- iommu/dma: Handle SG length overflow better
- usb: gadget: composite: Clear “suspended” on reset/disconnect
- usb: gadget: mass\_storage: Fix races between fsg\_disable and fsg\_set\_alt
- xen/blkback: fix memory leaks
- [arm64] cpufeature: Don’t treat granule sizes as strict
- drm/ast: Fixed reboot test may cause system hanged
- [x86] tools: hv: fix KVP and VSS daemons exit code
- [x86] drm/i915: fix broadwell EU computation
- [arm\*] watchdog: bcm2835\_wdt: Fix module autoload
- scsi: ufs: Fix RX\_TERMINATION\_FORCE\_ENABLE define value
- [armhf] drm/tilcdc: Register cpufreq notifier after we have initialized crtc
- ipv6/addrconf: allow adding multicast addr if IFA\_F\_MCAUTOJOIN is set
- ipv6: Default fib6\_type to RTN\_UNICAST when not set
- net/smc: make sure EPOLLOUT is raised
- tcp: make sure EPOLLOUT wont be missed
- ipv4/icmp: fix rt dst dev null pointer dereference
- mm/zsmalloc.c: fix build when CONFIG\_COMPACTON=n
- ALSA: usb-audio: Check mixer unit bitmap yet more strictly
- ALSA: line6: Fix memory leak at line6\_init\_pcm() error path
- ALSA: hda - Fixes inverted Conexant GPIO mic mute led
- ALSA: seq: Fix potential concurrent access to the deleted pool
- ALSA: usb-audio: Fix invalid NULL check in snd\_emuusb\_set\_samplerate()
- ALSA: usb-audio: Add implicit fb quirk for Behringer UFX1604
- [x86] kvm: skip populating logical dest map if apic is not sw enabled
- [x86] KVM: Don’t update RIP or do single-step on faulting emulation
- [amd64] uprobes: Fix detection of 32-bit user mode
- [x86] apic: Do not initialize LDR and DFR for bigsmp
- ftrace: Fix NULL pointer dereference in t\_probe\_next()
- ftrace: Check for successful allocation of hash
- ftrace: Check for empty hash and comment the race with registering probes
- usb-storage: Add new JMS567 revision to unusual\_devs
- USB: cdc-wdm: fix race between write and disconnect due to flag abuse
- usb: hcd: use managed device resources
- [armhf,arm64] usb: chipidea: udc: don’t do hardware access if gadget has stopped

- usb: host: ohci: fix a race condition between shutdown and irq
- usb: host: xhci: rcar: Fix typo in compatible string matching
- USB: storage: ums-realtek: Update module parameter description for auto\_delink\_en
- USB: storage: ums-realtek: Whitelist auto-delink support
- [x86] mei: me: add Tiger Lake point LP device ID
- mmc: core: Fix init of SD cards reporting an invalid VDD range
- stm class: Fix a double free of stm\_source\_device
- [x86] intel\_th: pci: Add support for another Lewisburg PCH
- [x86] intel\_th: pci: Add Tiger Lake support
- [x86] typec: tcpm: fix a typo in the comparison of pdo\_max\_voltage
- lib: logic\_pio: Fix RCU usage
- lib: logic\_pio: Avoid possible overlap for unregistering regions
- lib: logic\_pio: Add logic\_pio\_unregister\_range()
- [x86] drm/amdgpu: Add APTX quirk for Dell Latitude 5495
- [x86] drm/i915: Don't deballoon unused ggtt drm\_mm\_node in linux guest
- [x86] drm/i915: Call dma\_set\_max\_seg\_size() in i915\_driver\_hw\_probe()
- [arm64] bus: hisi\_lpc: Unregister logical PIO range to avoid potential use-after-free
- [arm64] bus: hisi\_lpc: Add .remove method to avoid driver unbind crash
- [x86] VMCI: Release resource if the work is already queued
- [x86] crypto: ccp - Ignore unconfigured CCP device on suspend/resume
- Revert "cfg80211: fix processing world regdomain when non modular"
- mac80211: fix possible sta leak
- mac80211: Don't memset RXCB prior to PAE intercept
- mac80211: Correctly set noencrypt for PAE frames
- [ppc64el] KVM: Book3S: Fix incorrect guest-to-user-translation error handling
- [armhf,arm64] KVM: vgic: Fix potential deadlock when ap\_list is long
- [armhf,arm64] KVM: vgic-v2: Handle SGI bits in GICD\_I{S,C}PENDR0 as WI
- NFS: Clean up list moves of struct nfs\_page
- NFSv4/pnfs: Fix a page lock leak in nfs\_pageio\_resend()
- NFS: Pass error information to the pgio error cleanup routine
- NFS: Ensure O\_DIRECT reports an error if the bytes read/written is 0
- [x86] i2c: piix4: Fix port selection for AMD Family 16h Model 30h
- mt76: mt76x0u: do not reset radio on resume

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.71>

- Revert "Input: elantech - enable SMBus on new (2018+) systems" (regression in 4.19.67)

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.72>



- mld: fix memory leak in mld\_del\_delrec()
- net: fix skb use after free in netpoll
- net: sched: act\_sample: fix psample group handling on overwrite
- net\_sched: fix a NULL pointer deref in ipt action
- [armhf,arm64] net: stmmac: dwmac-rk: Don't fail if phy regulator is absent
- tcp: inherit timestamp on mtu probe
- tcp: remove empty skb from write queue in error cases
- net/rds: Fix info leak in rds6\_inc\_info\_copy() (CVE-2019-16714)
- [x86] boot: Preserve boot\_params.secure\_boot from sanitizing
- [arm\*] spi: bcm2835aux: unifying code between polling and interrupt driven code
- [arm\*] spi: bcm2835aux: remove dangerous uncontrolled read of fifo
- [arm\*] spi: bcm2835aux: fix corruptions for longer spi transfers
- netfilter: nf\_tables: use-after-free in failing rule with bound set
- [x86] hv\_netvsc: Fix a warning of suspicious RCU usage
- Bluetooth: btqca: Add a short delay before downloading the NVM
- [ppc64el] ibmveth: Convert multicast list size for little-endian system
- gpio: Fix build error of function redefinition
- netfilter: nft\_flow\_offload: skip tcp rst and fin packets
- scsi: qla2xxx: Fix gnl.l memory leak on adapter init failure
- scsi: target: tcmu: avoid use-after-free after command timeout
- cxgb4: fix a memory leak bug
- liquidio: add cleanup in octeon\_setup\_iq()
- net: myri10ge: fix memory leaks
- lan78xx: Fix memory leaks
- vfs: fix page locking deadlocks when deduping files
- cx82310\_eth: fix a memory leak bug
- net: kalmia: fix memory leaks
- net: cavium: fix driver name
- wimax/i2400m: fix a memory leak bug
- kprobes: Fix potential deadlock in kprobe\_optimizer()
- HID: cp2112: prevent sleeping function called from invalid context
- [amd64] boot/compressed: Fix boot on machines with broken E820 table
- [x86] Input: hyperv-keyboard: Use in-place iterator API in the channel callback
- [x86] Tools: hv: kvp: eliminate 'may be used uninitialized' warning
- nvme-multipath: fix possible I/O hang when paths are updated
- IB/mlx4: Fix memory leaks

- infiniband: hfi1: fix a memory leak bug
- infiniband: hfi1: fix memory leaks
- ceph: fix buffer free while holding i\_ceph\_lock in \_\_ceph\_setxattr()
- ceph: fix buffer free while holding i\_ceph\_lock in \_\_ceph\_build\_xattrs\_blob()
- ceph: fix buffer free while holding i\_ceph\_lock in fill\_inode()
- [armhf,arm64] KVM: Only skip MMIO insn once
- afs: Fix leak in afs\_lookup\_cell\_rcu()
- [armhf,arm64] KVM: VGIC: Properly initialise private IRQ affinity
- [amd64] boot/compressed: Fix missing initialization in find\_trampoline\_placement()
- libceph: allow ceph\_buffer\_put() to receive a NULL ceph\_buffer

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.73>

- ALSA: hda - Fix potential endless loop at applying quirks
- ALSA: hda/realtek - Fix overridden device-specific initialization
- [x86] ALSA: hda/realtek - Add quirk for HP Pavilion 15
- [x86] ALSA: hda/realtek - Enable internal speaker & headset mic of ASUS UX431FL
- [x86] ALSA: hda/realtek - Fix the problem of two front mics on a ThinkCentre
- sched/fair: Don't assign runtime for throttled cfs\_rq
- [x86] drm/vmwgfx: Fix double free in vmw\_recv\_msg()
- [ppc64el] tm: Fix FP/VMX unavailable exceptions inside a transaction (CVE-2019-15030)
- batman-adv: fix uninit-value in batadv\_netlink\_get\_ifindex()
- batman-adv: Only read OGM tvlv\_len after buffer len check
- [x86] hv\_sock: Fix hang when a connection is closed
- blk-iolatency: warn on negative inflight IO counter
- blk-iolatency: fix STS\_AGAIN handling
- {nl,mac}80211: fix interface combinations on crypto controlled devices
- timekeeping: Use proper ktime\_add when adding nsecs in coarse offset
- selftests: fib\_rule\_tests: use pre-defined DEV\_ADDR
- [x86] ftrace: Fix warning and consolidate ftrace\_jump\_replace() and ftrace\_call\_replace()
- [ppc64el] mark start\_here\_multiplatform as \_\_ref
- [arm64] dts: rockchip: enable usb-host regulators at boot on rk3328-rock64
- nvme-fc: use separate work queue to avoid warning
- [armhf] clk: s2mps11: Add used attribute to s2mps11\_dt\_match
- [arm64] remoteproc: qcom: q6v5: shore up resource probe handling
- modules: always page-align module section allocations
- kernel/module: Fix mem leak in module\_add\_modinfo\_attrs
- [x86] drm/i915: Re-apply "Perform link quality check, unconditionally during long pulse"

- scsi: qla2xxx: Move log messages before issuing command to firmware
- keys: Fix the use of the C++ keyword “private” in uapi/linux/keyctl.h
- [x86] Drivers: hv: kvp: Fix two “this statement may fall through” warnings
- [x86] hibernate: Fix nosave\_regions setup for hibernation
- [arm64] remoteproc: qcom: q6v5-mss: add SCM probe dependency
- drm/amdgpu/gfx9: Update gfx9 golden settings.
- drm/amdgpu: Update gc\_9\_0 golden settings.
- [x86] KVM: hyperv: enforce vp\_index < KVM\_MAX\_VCPU
- [x86] KVM: hyperv: consistently use ‘hv\_vcpu’ for ‘struct kvm\_vcpu\_hv’ variables
- [x86] KVM: hyperv: keep track of mismatched VP indexes
- [x86] KVM: hyperv: define VP assist page helpers
- [x86] kvm/lapic: preserve gfn\_to\_hva\_cache len on cache reinit
- [x86] drm/i915: Fix intel\_dp\_mst\_best\_encoder()
- [x86] drm/i915: Rename PLANE\_CTL\_DECOMPRESSION\_ENABLE
- [x86] drm/i915/gen9+: Fix initial readout for Y tiled framebuffers
- drm/atomic\_helper: Disallow new modesets on unregistered connectors
- [x86] Drivers: hv: kvp: Fix the recent regression caused by incorrect clean-up
- powerplay: Respect units on max dcfclk watermark
- drm/amd/pp: Fix truncated clock value when set watermark
- drm/amd/dm: Understand why attaching path/tile properties are needed
- [s390x] zcrypt: reinit ap queue state machine during device probe
- [x86] drm/i915: Restore sane defaults for KMS on GEM error load
- [x86] drm/i915: Cleanup gt powerstate from gem
- [ppc64el] KVM: Book3S HV: Fix race between kvm\_unmap\_hva\_range and MMU mode switch
- Btrfs: clean up scrub is\_dev\_replace parameter
- Btrfs: fix deadlock with memory reclaim during scrub
- btrfs: Remove extent\_io\_ops::fill\_delalloc
- btrfs: Fix error handling in btrfs\_cleanup\_ordered\_extents
- scsi: megaraid\_sas: Fix combined reply queue mode detection
- scsi: megaraid\_sas: Add check for reset adapter bit
- scsi: megaraid\_sas: Use 63-bit DMA addressing
- [ppc64el] pkeys: Fix handling of pkey state across fork()
- btrfs: volumes: Make sure no dev extent is beyond device boundary
- btrfs: Use real device structure to verify dev extent
- IB/uverbs: Fix OOPs upon device disassociation
- drm/vblank: Allow dynamic per-crtc max\_vblank\_count

- [x86] drm/i915/ilk: Fix warning when reading emon\_status with no output
- tpm: Fix some name collisions with drivers/char/tpm.h
- bcache: replace hard coded number with BUCKET\_GC\_GEN\_MAX
- bcache: treat stale && dirty keys as bad keys
- [x86] KVM: VMX: Compare only a single byte for VMCS' "launched" in vCPU-run
- [armhf] iio: adc: exynos-adc: Add S5PV210 variant
- [armhf] iio: adc: exynos-adc: Use proper number of channels for Exynos4x12
- mt76: fix corrupted software generated tx CCMP PN
- drm/nouveau: Don't WARN\_ON VCPI allocation failures
- iwlfwifi: fix devices with PCI Device ID 0x34F0 and 11ac RF modules
- iwlfwifi: add new card for 9260 series
- spi: spi-gpio: fix SPI\_CS\_HIGH capability
- [ppc64el] kvm: Save and restore host AMR/IAMR/UAMOR
- btrfs: scrub: pass fs\_info to scrub\_setup\_ctx
- btrfs: scrub: move scrub\_setup\_ctx allocation out of device\_list\_mutex
- btrfs: scrub: fix circular locking dependency warning
- btrfs: init csum\_list before possible free
- [arm64] PCI: qcom: Fix error handling in runtime PM support
- [arm64] PCI: qcom: Don't deassert reset GPIO during probe
- CIFS: Fix error paths in writeback code
- CIFS: Fix leaking locked VFS cache pages in writeback retry
- [x86] drm/i915: Handle vm\_mmap error during I915\_GEM\_MMAP ioctl with WC set
- [x86] drm/i915: Sanity check mmap length against object size
- [x86] usb: typec: tcpm: Try PD-2.0 if sink does not respond to 3.0 source-caps
- IB/mlx5: Reset access mask when looping inside page fault handler
- kvm: mmu: Fix overflow on kvm mmu page limit calculation
- [x86] kvm: move kvm\_load/put\_guest\_xcr0 into atomic context
- [x86] KVM: Always use 32-bit SMRAM save state for 32-bit kernels
- cifs: Fix lease buffer length error (CVE-2019-15918)
- ext4: protect journal inode's blocks using block\_validity
- [x86] PCI: Reset Lenovo ThinkPad P50 nvgpu at boot if necessary
- dm mpath: fix missing call of path selector type->end\_io
- blk-mq: free hw queue's resource in hctx's release handler
- mmc: sdhci-pci: Add support for Intel CML
- PCI: dwc: Use devm\_pci\_alloc\_host\_bridge() to simplify code
- cifs: smbdc: take an array of requests when sending upper layer data

- dm crypt: move detailed message into debug level
- [x86] drm/amdkfd: Add missing Polaris10 ID
- kvm: Check irqchip mode before assign irqfd
- drm/amdgpu: fix ring test failure issue during s3 in vce 3.0 (V2)
- drm/amdgpu/{uvd,vcn}: fetch ring's read\_ptr after alloc
- Btrfs: fix race between block group removal and block group allocation
- cifs: add spinlock for the openFileList to cifsInodeInfo
- [arm64] clk: tegra: Fix maximum audio sync clock for Tegra124/210
- [arm64] clk: tegra210: Fix default rates for HDA clocks
- IB/hfi1: Avoid hardlockup with flushlist\_lock
- apparmor: reset pos on failure to unpack for various functions
- scsi: target/core: Use the SECTOR\_SHIFT constant
- scsi: target/iblock: Fix overrun in WRITE SAME emulation
- [s390x] scsi: zfcp: fix request object use-after-free in send path causing wrong traces
- cifs: Properly handle auto disabling of serverino option
- [x86] ALSA: hda - Don't resume forcibly i915 HDMI/DP codec
- [x86] KVM: optimize check for valid PAT value
- [x86] KVM: VMX: Always signal #GP on WRMSR to MSR\_IA32\_CR\_PAT with bad value
- [x86] KVM: VMX: Fix handling of #MC that occurs during VM-Entry
- [x86] KVM: VMX: check CPUID before allowing read/write of IA32\_XSS
- [ppc64el] KVM: Use ccr field in pt\_regs struct embedded in vcpu struct
- [ppc64el] KVM: Book3S HV: Fix CR0 setting in TM emulation
- RDMA/srp: Document srp\_parse\_in() arguments
- RDMA/srp: Accept again source addresses that do not have a port number
- btrfs: correctly validate compression type
- resource: Include resource end in walk\_\*() interfaces
- resource: Fix find\_next\_iomem\_res() iteration issue
- resource: fix locking in find\_next\_iomem\_res()
- pstore: Fix double-free in pstore\_mkfile() failure path
- dm thin metadata: check if in fail\_io mode when setting needs\_check
- [armhf,arm64] drm/panel: Add support for Armadeus ST0700 Adapt
- [x86] ALSA: hda - Fix intermittent CORB/RIRB stall on Intel chips
- [ppc64el] mm: Limit rma\_size to 1TB when running without HV mode
- iommu/iova: Remove stale cached32\_node
- gpio: don't WARN() on NULL descs if gpiolib is disabled
- mm/migrate.c: initialize pud\_entry in migrate\_vma()

- NFSv4: Fix delegation state recovery
- bcache: only clear BTREE\_NODE\_dirty bit when it is set
- bcache: add comments for mutex\_lock(&b->write\_lock)
- bcache: fix race in btree\_flush\_write()
- [x86] drm/i915: Make sure cdclk is high enough for DP audio on VLV/CHV
- [s390x] virtio: fix race on airq\_areas[]
- drm/atomic\_helper: Allow DPMS On<->Off changes for unregistered connectors
- ext4: don't perform block validity checks on the journal inode
- ext4: fix block validity checks for journal inodes using indirect blocks
- ext4: unsigned int compared against zero
- [x86] PCI: Reset both NVIDIA GPU and HDA in ThinkPad P50 workaround
- [ppc64el] tm: Remove msr\_tm\_active()
- [ppc64el] tm: Fix restoring FP/VMX facility incorrectly on interrupts (CVE-2019-15031)

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.74>

- bridge/mdb: remove wrong use of NLM\_F\_MULTI
- cdc\_ether: fix rndis support for Mediatek based smartphones
- ipv6: Fix the link time qualifier of 'ping\_v6\_proc\_exit\_net()'
- isdn/capi: check message length in capi\_write()
- net: Fix null de-reference of device refcount
- net: gso: Fix skb\_segment splat when splitting gso\_size mangled skb having linear-headed frag\_list
- net: phylink: Fix flow control resolution
- net: sched: fix reordering issues
- sch\_hhf: ensure quantum and hhf\_non\_hh\_weight are non-zero
- sctp: Fix the link time qualifier of 'sctp\_ctrlsock\_exit()'
- sctp: use transport pf\_retrans in sctp\_do\_8\_2\_transport\_strike
- tcp: fix tcp\_ecn\_withdraw\_cwr() to clear TCP\_ECN\_QUEUE\_CWR
- tipc: add NULL pointer check before calling kfree\_rcu
- tun: fix use-after-free when register netdev failed
- gpiolib: acpi: Add gpiolib\_acpi\_run\_edge\_events\_on\_boot option and blacklist
- gpio: fix line flag validation in linehandle\_create
- Btrfs: fix assertion failure during fsync and use of stale transaction
- ixgbe: Prevent u8 wrapping of ITR value to something less than 10us
- genirq: Prevent NULL pointer dereference in resend\_irqs()
- [s390x] KVM: kvm\_s390\_vm\_start\_migration: check dirty\_bitmap before using it as target for memset()
- [s390x] KVM: Do not leak kernel stack data in the KVM\_S390\_INTERRUPT ioctl
- [x86] KVM: work around leak of uninitialized stack contents

- [x86] KVM: nVMX: handle page fault in vmread
- [x86] purgatory: Change compiler flags from -mcmmodel=kernel to -mcmmodel=large to fix kexec relocation errors
- [ppc64el] Add barrier\_nospec to raw\_copy\_in\_user()
- [arm64] drm/meson: Add support for XBGR8888 & ABGR8888 formats
- [armhf,arm64] clk: rockchip: Don't yell about bad mmc phases when getting
- PCI: Always allow probing with driver\_override
- gpio: fix line flag validation in lineevent\_create
- ubifs: Correctly use tnc\_next() in search\_dh\_cookie()
- driver core: Fix use-after-free and double free on glue directory
- firmware: ti\_sci: Always request response from firmware
- [x86] drm: panel-orientation-quirks: Add extra quirk table entry for GPD MicroPC
- Revert "Bluetooth: btusb: driver to enable the usb-wakeup feature"
- modules: fix BUG when load module with rodata=n
- rsi: fix a double free bug in rsi\_91x\_deinit() (CVE-2019-15504)
- nvme: Use the same permissions for eeprom as for nvme

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.75>

- netfilter: nf\_flow\_table: set default timeout after successful insertion
- HID: wacom: generic: read HID\_DG\_CONTACTMAX from any feature report
- RDMA/restrack: Release task struct which was hold by CM\_ID object
- [x86] Input: elan\_i2c - remove Lenovo Legion Y7000 PnpID
- [ppc64el] mm/radix: Use the right page size for vmemmap mapping
- USB: usbcore: Fix slab-out-of-bounds bug during device reset
- media: tm6000: double free if usb disconnect while streaming
- ip6\_gre: fix a dst leak in ip6erspan\_tunnel\_xmit
- udp: correct reuseport selection with connected sockets
- xen-netfront: do not assume sk\_buff\_head list is empty in error handling
- net\_sched: let qdisc\_put() accept NULL pointer
- mwifiex: Fix three heap overflow at parsing element in cfg80211\_ap\_settings (CVE-2019-14814, CVE-2019-14815, CVE-2019-14816)
- nl80211: Fix possible Spectre-v1 for CQM RSSI thresholds
- ieee802154: hwsim: Fix error handle path in hwsim\_init\_module
- ieee802154: hwsim: unregister hw while hwsim\_subscribe\_all\_others fails
- [armhf] dts: am57xx: Disable voltage switching for SD card
- [armhf] OMAP2+: Fix missing SYSC\_HAS\_RESET\_STATUS for dra7 epwmss
- [armhf] bus: ti-sysc: Fix using configured sysc mask value
- [s390x] bpf: fix lcg instruction encoding

- [armhf] OMAP2+: Fix omap4 errata warning on other SoCs
- [armhf] dts: dra74x: Fix iodelay configuration for mmc3
- [armhf] bus: ti-sysc: Simplify cleanup upon failures in sysc\_probe()
- [s390x] bpf: use 32-bit index for tail calls
- netfilter: ebttables: Fix argument order to ADD\_COUNTER
- netfilter: nft\_flow\_offload: missing netlink attribute policy
- netfilter: xt\_nfacct: Fix alignment mismatch in xt\_nfacct\_match\_info
- NFSv4: Fix return values for nfs4\_file\_open()
- NFSv4: Fix return value in nfs\_finish\_open()
- NFS: Fix initialisation of I/O result struct in nfs\_pgio\_rpcsetup
- xdp: unpin xdp umem pages in error path
- qed: Add cleanup in qed\_slowpath\_start()
- [armel,armhf] 8874/1: mm: only adjust sections of valid mm structures
- batman-adv: Only read OGM2 tvlv\_len after buffer len check
- bpf: allow narrow loads of some sk\_reuseport\_md fields with offset > 0
- r8152: Set memory to all 0xFFs on failed reg reads
- [x86] apic: Fix arch\_dynirq\_lower\_bound() bug for DT enabled machines
- netfilter: xt\_physdev: Fix spurious error message in physdev\_mt\_check
- netfilter: nf\_conntrack\_ftp: Fix debug output
- NFSv2: Fix eof handling
- NFSv2: Fix write regression
- kallsyms: Don't let kallsyms\_lookup\_size\_offset() fail on retrieving the first symbol
- cifs: set domainName when a domain-key is used in multiuser
- cifs: Use kzfree() to zero out the password
- [armhf,arm64] usb: host: xhci-tegra: Set DMA mask correctly
- [armel,armhf] 8901/1: add a criteria for pfn\_valid of arm
- sky2: Disable MSI on yet another ASUS boards (P6Xxxx)
- i2c: designware: Synchronize IRQs when unregistering slave client
- [x86] perf/intel: Restrict period on Nehalem
- [x86] perf/amd/ibs: Fix sample bias for dispatched micro-ops
- amd-xgbe: Fix error path in xgbe\_mod\_init()
- [x86] tools/power x86\_energy\_perf\_policy: Fix argument parsing
- [x86] tools/power turbostat: fix buffer overrun
- net: aquantia: fix out of memory condition on rx side
- [armhf] dmaengine: ti: omap-dma: Add cleanup in omap\_dma\_probe()
- [x86] uaccess: Don't leak the AC flags into \_\_get\_user() argument evaluation



- [x86] hyper-v: Fix overflow bug in fill\_gva\_list()
- keys: Fix missing null pointer check in request\_key\_auth\_describe()
- [x86] iommu/amd: Flush old domains in kdump kernel
- [x86] iommu/amd: Fix race in increase\_address\_space()
- [arm64] PCI: kirin: Fix section mismatch warning
- ovl: fix regression caused by overlapping layers detection
- floppy: fix usercopy direction
- binfmt\_elf: move brk out of mmap when doing direct loader exec
- [arm64] kpti: Whitelist Cortex-A CPUs that don't implement the CSV3 field
- media: technisat-usb2: break out of loop at end of buffer (CVE-2019-15505)

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.76>

- Revert "Bluetooth: validate BLE connection interval updates"
- RDMA/restrack: Protect from reentry to resource return path
- [ppc64el] xive: Fix bogus error code returned by OPAL
- IB/core: Add an unbound WQ type to the new CQ API
- HID: prodikeys: Fix general protection fault during probe
- HID: sony: Fix memory corruption issue on cleanup.
- HID: logitech: Fix general protection fault caused by Logitech driver
- HID: hidraw: Fix invalid read in hidraw\_ioctl
- HID: Add quirk for HP X500 PIXART OEM mouse
- mtd: cfi\_cmdset\_0002: Use chip\_good() to retry in do\_write\_oneword()
- CIFS: fix deadlock in cached root handling
- net/mlx5e: Set ECN for received packets using CQE indication
- net/mlx5e: don't set CHECKSUM\_COMPLETE on SCTP packets
- mlx5: fix get\_ip\_proto()
- net/mlx5e: Allow reporting of checksum unnecessary
- net/mlx5e: XDP, Avoid checksum complete when XDP prog is loaded
- net/mlx5e: Rx, Fixup skb checksum for packets with tail padding
- net/mlx5e: Rx, Check ip headers sanity
- iwlfwifi: mvm: send BCAST management frames to the right station
- iwlfwifi: mvm: always init rs\_fw with 20MHz bandwidth rates
- media: tvp5150: fix switch exit in set control handler
- [x86] ASoC: Intel: cht\_bsw\_max98090\_ti: Enable codec clock once and keep it enabled
- ALSA: usb-audio: Add Hiby device family to quirks for native DSD support
- ALSA: usb-audio: Add DSD support for EVGA NU Audio
- ALSA: dice: fix wrong packet parameter for Alesis iO26

- [x86] ALSA: hda - Add laptop imic fixup for ASUS M9V laptop
- [x86] ALSA: hda - Apply AMD controller workaround for Raven platform
- objtool: Clobber user CFLAGS variable
- power: supply: sysfs: ratelimit property read error message
- scsi: qla2xxx: Turn off IOCB timeout timer on IOCB completion
- scsi: qla2xxx: Remove all rports if fabric scan retry fails
- scsi: qla2xxx: Return switch command on a timeout
- Revert "drm/amd/powerplay: Enable/Disable NBPSTATE on On/OFF of UVD"
- bpf: libbpf: retry loading program on EAGAIN
- [armhf,arm64] irqchip/gic-v3-its: Fix LPI release for Multi-MSI devices
- f2fs: check all the data segments against all node ones
- [x86] PCI: hv: Avoid use of hv\_pci\_dev->pci\_slot after freeing it
- bcache: remove redundant LIST\_HEAD(journal) from run\_cache\_set()
- initramfs: don't free a non-existent initrd
- blk-mq: change gfp flags to GFP\_NOIO in blk\_mq\_realloc\_hw\_ctxs
- blk-mq: move cancel of requeue\_work to the front of blk\_exit\_queue
- Revert "f2fs: avoid out-of-range memory access"
- dm zoned: fix invalid memory access
- f2fs: fix to do sanity check on segment bitmap of LFS curseg
- drm: Flush output polling on shutdown
- net: don't warn in inet diag when IPV6 is disabled
- Bluetooth: btrtl: HCI reset on close for Realtek BT chip
- [x86] ACPI: video: Add new hw\_changes\_brightness quirk, set it on PB Easynote MZ35
- drm/nouveau/disp/nv50-: fix center/aspect-corrected scaling
- xfs: don't crash on null attr fork xfs\_bmapi\_read
- netfilter: nft\_socket: fix erroneous socket assignment
- Bluetooth: btrtl: Additional Realtek 8822CE Bluetooth devices
- net\_sched: check cops->tcf\_block in tc\_bind\_tclass()
- net/rds: An rds\_sock is added too early to the hash table
- net/rds: Check laddr\_check before calling it
- f2fs: use generic EFSBADCRC/EFSCORRUPTED

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.77>

- arcnet: provide a buffer big enough to actually receive packets
- cdc\_ncm: fix divide-by-zero caused by invalid wMaxPacketSize
- macsec: drop skb sk before calling gro\_cells\_receive
- net/phy: fix DP83865 10 Mbps HDX loopback disable function

- net/sched: act\_sample: don't push mac header on ip6gre ingress
- net\_sched: add max len check for TCA\_KIND
- nfp: flower: fix memory leak in nfp\_flower\_spawn\_vnic\_reprs (CVE-2019-19081)
- openvswitch: change type of UPCALL\_PID attribute to NLA\_UNSPEC
- ppp: Fix memory leak in ppp\_write
- sch\_netem: fix a divide by zero in tabledist()
- skge: fix checksum byte order
- usbnet: ignore endpoints with invalid wMaxPacketSize
- usbnet: sanity checking of packet sizes and device mtu
- net: sched: fix possible crash in tcf\_action\_destroy()
- tcp: better handle TCP\_USER\_TIMEOUT in SYN\_SENT state
- net/mlx5: Add device ID of upcoming BlueField-2
- mISDN: enforce CAP\_NET\_RAW for raw sockets (CVE-2019-17055)
- appletalk: enforce CAP\_NET\_RAW for raw sockets (CVE-2019-17054)
- ax25: enforce CAP\_NET\_RAW for raw sockets (CVE-2019-17052)
- ieee802154: enforce CAP\_NET\_RAW for raw sockets (CVE-2019-17053)
- nfc: enforce CAP\_NET\_RAW for raw sockets (CVE-2019-17056)
- nfp: flower: prevent memory leak in nfp\_flower\_spawn\_phy\_reprs (CVE-2019-19080)
- ALSA: hda: Flush interrupts on disabling
- [armhf] ASoC: sgtl5000: Fix of unmute outputs on probe
- [armhf] ASoC: sgtl5000: Fix charge pump source assignment
- [arm\*] dmaengine: bcm2835: Print error in case setting DMA mask fails
- media: dib0700: fix link error for dibx000\_i2c\_set\_speed
- media: hdpvr: Add device num check and handling
- time/tick-broadcast: Fix tick\_broadcast\_offline() lockdep complaint
- sched/fair: Fix imbalance due to CPU affinity
- sched/core: Fix CPU controller for !RT\_GROUP\_SCHED
- [x86] apic: Make apic\_pending\_intr\_clear() more robust
- sched/deadline: Fix bandwidth accounting at all levels after offline migration
- [x86] reboot: Always use NMI fallback when shutdown via reboot vector IPI fails
- [x86] apic: Soft disable APIC before initializing it
- ALSA: hda - Show the fatal CORB/RIRB error more clearly
- ALSA: i2c: ak4xxx-adda: Fix a possible null pointer dereference in build\_adc\_controls()
- EDAC/mc: Fix grain\_bits calculation
- media: iguanair: add sanity checks
- base: soc: Export soc\_device\_register/unregister APIs

- ALSA: usb-audio: Skip bSynchAddress endpoint check if it is invalid
- [arm64] prefetch: fix a -Wtype-limits warning
- md/raid1: end bio when the device faulty
- md: don't call spare\_active in md\_reap\_sync\_thread if all member devices can't work
- md: don't set In\_sync if array is frozen
- ACPI / processor: don't print errors for processorIDs == 0xff
- loop: Add LOOP\_SET\_DIRECT\_IO to compat ioctl
- [x86] EDAC, pnd2: Fix ioremap() size in dnv\_rd\_reg()
- efi: cper: print AER info of PCIe fatal error
- sched/fair: Use rq\_lock/unlock in online\_fair\_sched\_group
- idle: Prevent late-arriving interrupts from disrupting offline
- media: gspca: zero usb\_buf on error
- perf config: Honour \$PERF\_CONFIG env var to specify alternate .perfconfig
- perf test vfs\_getname: Disable ~/.perfconfig to get default output
- media: em28xx: modules workqueue not inited for 2nd device
- media: rc: imon: Allow iMON RC protocol for ffdc 7e device
- [arm64] perf record: Support aarch64 random socket\_id assignment
- [armhf] media: omap3isp: Don't set streaming state on random subdevs
- media: radio/si470x: kill urb on error
- media: hdpvr: add terminating 0 at end of string
- led: triggers: Fix a memory leak bug
- nbd: add missing config put
- media: mceusb: fix (eliminate) TX IR signal length limit
- media: dvb-frontends: use ida for pll number
- posix-cpu-timers: Sanitize bogus WARNONS
- media: dvb-core: fix a memory leak bug
- libperf: Fix alignment trap with xyarray contents in 'perf stat'
- [amd64] EDAC/amd64: Recognize DRAM device type ECC capability
- [amd64] EDAC/amd64: Decode syndrome before translating address
- PM / devfreq: passive: Use non-devm notifiers
- PM / devfreq: exynos-bus: Correct clock enable sequence
- media: cec-notifier: clear cec\_adap in cec\_notifier\_unregister
- media: saa7146: add cleanup in hexium\_attach()
- media: cpia2\_usb: fix memory leaks
- media: saa7134: fix terminology around saa7134\_i2c\_eeprom\_md7134\_gate()
- perf trace beauty ioctl: Fix off-by-one error in cmd->string table

- [x86] ASoC: es8316: fix headphone mixer volume table
- ACPI / CPPC: do not require the \_PSD method
- sched/cpufreq: Align trace event behavior of fast switching
- [x86] apic/vector: Warn when vector space exhaustion breaks affinity
- [arm64] kpti: ensure patched kernel text is fetched from PoU
- [x86] mm/pti: Do not invoke PTI functions when PTI is disabled
- [x86] mm/pti: Handle unaligned address gracefully in pti\_clone\_pagetable()
- nvmet: fix data units read and written counters in SMART log
- nvme-multipath: fix ana log nsid lookup when nsid is not found
- ALSA: firewire-motu: add support for MOTU 4pre
- iommu/amd: Silence warnings under memory pressure
- libata/ahci: Drop PCS quirk for Denverton and beyond
- iommu/iova: Avoid false sharing on fq\_timer\_on
- libtraceevent: Change users plugin directory
- [armhf] dts: exynos: Mark LDO10 as always-on on Peach Pit/Pi Chromebooks
- ACPI: custom\_method: fix memory leaks
- ACPI / PCI: fix acpi\_pci\_irq\_enable() memory leak
- closures: fix a race on wakeup from closure\_sync
- hwmon: (acpi\_power\_meter) Change log level for 'unsafe software power cap'
- md/raid1: fail run raid1 array when active disk less than one
- dmaengine: ti: edma: Do not reset reserved paRAM slots
- kprobes: Prohibit probing on BUG() and WARN() address
- [s390x] crypto: xts-aes-s390 fix extra run-time crypto self tests finding
- [x86] cpu: Add Tiger Lake to Intel family
- [x86] platform: intel\_pmc\_core: Do not ioremap RAM
- ASoC: dmaengine: Make the pcm->name equal to pcm->id if the name is not set
- raid5: don't set STRIPE\_HANDLE to stripe which is in batch list
- mmc: core: Clarify sdio\_irq\_pending flag for MMC\_CAP2\_SDIO\_IRQ\_NOTHREAD
- mmc: sdhci: Fix incorrect switch to HS mode
- mmc: core: Add helper function to indicate if SDIO IRQs is enabled
- [armhf,arm64] mmc: dw\_mmc: Re-store SDIO IRQs mask at system resume
- raid5: don't increment read\_errors on EILSEQ return
- libertas: Add missing sentinel at end of if\_usb.c fw\_table
- e1000e: add workaround for possible stalled packet
- ALSA: hda - Drop unsol event handler for Intel HDMI codecs
- drm/amd/powerplay/smu7: enforce minimal VBITimeout (v2)

- media: ttusb-dec: Fix info-leak in ttusb\_dec\_send\_command()
- [x86] ALSA: hda/realtek - Blacklist PC beep for Lenovo ThinkCentre M73/93
- [x86] iommu/amd: Override wrong IVRS IOAPIC on Raven Ridge systems
- btrfs: extent-tree: Make sure we only allocate extents from block groups with the same type
- [armhf] media: omap3isp: Set device on omap3isp subdevs
- PM / devfreq: passive: fix compiler warning
- iwlfwifi: fw: don't send GEO\_TX\_POWER\_LIMIT command to FW version 36
- ALSA: firewire-tascam: handle error code when getting current source of clock
- ALSA: firewire-tascam: check intermediate state of clock status and retry
- scsi: scsi\_dh\_rdac: zero cdb in send\_mode\_select()
- scsi: qla2xxx: Fix Relogin to prevent modifying scan\_state flag
- printk: Do not lose last line in kmsg buffer dump
- IB/mlx5: Free mpi in mp\_slave mode
- IB/hfi1: Define variables as unsigned long to fix KASAN warning
- randstruct: Check member structs in is\_pure\_ops\_struct()
- ceph: use ceph\_evict\_inode to cleanup inode's resource
- [x86] ALSA: hda/realtek - PCI quirk for Medion E4254
- blk-mq: add callback of .cleanup\_rq
- scsi: implement .cleanup\_rq callback
- [ppc64el] imc: Dont create debugfs files for cpu-less nodes
- fuse: fix missing unlock\_page in fuse\_writepage()
- [x86] KVM: always stop emulation on page fault
- [x86] KVM: set ctxt->have\_exception in x86\_decode\_insn()
- [x86] KVM: Manually calculate reserved bits when loading PDPTRS
- [x86] media: sn9c20x: Add MSI MS-1039 laptop to flip\_dmi\_table
- media: don't drop front-end reference count for ->detach
- binfmt\_elf: Do not move brk for INTERP-less ET\_EXEC
- [x86] ASoC: Intel: NHLT: Fix debug print format
- [x86] ASoC: Intel: Skylake: Use correct function to access iomem space
- [x86] ASoC: Intel: Fix use of potentially uninitialized variable
- [arm64] Revert "arm64: Remove unnecessary ISBs from set\_{pte,pmd,pud}"
- [arm64] tlb: Ensure we execute an ISB following walk cache invalidation
- [arm64] dts: rockchip: limit clock rate of MMC controllers for RK3328
- alarmtimer: Use EOPNOTSUPP instead of ENOTSUPP
- regulator: Defer init completion for a while after late\_initcall
- efifb: BGRT: Improve efifb\_bgrt\_sanity\_check

- gfs2: clear buf\_in\_tr when ending a transaction in sweep\_bh\_for\_rgrps
- memcg, oom: don't require \_\_GFP\_FS when invoking memcg OOM killer
- memcg, kmem: do not fail \_\_GFP\_NOFAIL charges
- i40e: check \_\_I40E\_VF\_DISABLE bit in i40e\_sync\_filters\_subtask
- block: fix null pointer dereference in blk\_mq\_rq\_timed\_out()
- smb3: allow disabling requesting leases
- ovl: Fix dereferencing possible ERR\_PTR()
- ovl: filter of trusted xattr results in audit
- btrfs: fix allocation of free space cache v1 bitmap pages
- Btrfs: fix use-after-free when using the tree modification log
- btrfs: Relinquish CPUs in btrfs\_compare\_trees
- btrfs: qgroup: Fix the wrong target io\_tree when freeing reserved data space
- btrfs: qgroup: Fix reserved data space leak if we have multiple reserve calls
- Btrfs: fix race setting up and completing qgroup rescan workers
- md/raid6: Set R5\_ReadError when there is read failure on parity disk
- md: don't report active array\_state until after revalidate\_disk() completes.
- md: only call set\_in\_sync() when it is expected to succeed.
- cfg80211: Purge frame registrations on iftype change
- /dev/mem: Bail out upon SIGKILL.
- ext4: fix warning inside ext4\_convert\_unwritten\_extents\_endio
- ext4: fix punch hole for inline\_data file systems
- quota: fix wrong condition in is\_quota\_modification()
- hwng: core - don't wait on add\_early\_randomness()
- CIFS: fix max ea value size
- CIFS: Fix oplock handling for SMB 2.1+ protocols
- md/raid0: avoid RAID0 data corruption due to layout confusion.
- fuse: fix deadlock with aio poll and fuse\_iqueue::waitq.lock
- mm/compaction.c: clear total\_{migrate,free}\_scanned before scanning a new zone
- drm/amd/display: Restore backlight brightness after system resume

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.78>

- tpm: use tpm\_try\_get\_ops() in tpm-sysfs.c.
- tpm: Fix TPM 1.2 Shutdown sequence to prevent future TPM operations
- [armhf,arm64] drm/panel: simple: fix AUO g185han01 horizontal blanking
- [armhf,arm64] drm/panel: check failure cases in the probe func
- [armhf,arm64] drm/rockchip: Check for fast link training before enabling psr
- gpu: drm: radeon: Fix a possible null-pointer dereference in radeon\_connector\_set\_property()

- [ppc64el] PCI: rpaphp: Avoid a sometimes-uninitialized warning
- ipmi\_si: Only schedule continuously in the thread in maintenance mode
- [armhf,arm64] clk: sunxi-ng: v3s: add missing clock slices for MMC2 module clocks
- drm/amd/display: fix issue where 252-255 values are clipped
- drm/amd/display: reprogram VM config when system resume
- [ppc64el] powernv/ioda2: Allocate TCE table levels on demand for default DMA window
- [ppc64el] xmon: Check for HV mode when dumping XIVE info from OPAL
- [ppc64el] rtas: use device model APIs and serialization during LPM
- [ppc64el] futex: Fix warning: 'oldval' may be used uninitialized in this function
- [ppc64el] pseries/mobility: use cond\_resched when updating device tree
- [armhf,arm64] pinctrl: tegra: Fix write barrier placement in pmx\_writel
- [ppc64el] eeh: Clear stale EEH\_DEV\_NO\_HANDLER flag
- vfio\_pci: Restore original state on release
- drm/nouveau/volt: Fix for some cards having 0 maximum voltage
- [x86] pinctrl: amd: disable spurious-firing GPIO IRQs
- drm/amd/display: support spdif
- drm/amdgpu/si: fix ASIC tests
- [ppc64el] exception: machine check use correct cfar for late handler
- pstore: fs superblock limits
- [ppc64el] pseries: correctly track irq state in default idle
- [arm64] pinctrl: meson-gxbb: Fix wrong pinning definition for uart\_c
- [ppc64el] dump kernel log before carrying out fadump or kdump
- [arm64] mbox: qcom: add APCS child device for QCS404
- scsi: core: Reduce memory required for SCSI logging
- dma-buf/sw\_sync: Synchronize signal vs syncpt free
- ext4: fix potential use after free after remounting with noblock\_validity
- [mips\*] tbex: Explicitly cast \_PAGE\_NO\_EXEC to a boolean
- [x86] i2c-cht-wc: Fix lockdep warning
- [x86] mfd: intel-lpss: Remove D3cold delay
- HID: wacom: Fix several minor compiler warnings
- [armel,armhf] 8898/1: mm: Don't treat faults reported from cache maintenance as writes
- [armhf] rtc: snvs: fix possible race condition
- HID: apple: Fix stuck function keys when using FN
- [arm64] PCI: rockchip: Propagate errors for optional regulators
- [armhf] PCI: imx6: Propagate errors for optional regulators
- [armel,armhf] 8903/1: ensure that usable memory in bank 0 starts from a PMD-aligned address



- fat: work around race with userspace's read via blockdev while mounting
- pktcdvd: remove warning on attempting to register non-passthrough dev
- [s390x] hypfs: Fix error number left in struct pointer member
- ocfs2: wait for recovering done after direct unlock request
- [arm64] consider stack randomization for mmap base only when necessary
- [mips\*] properly account for stack randomization and stack guard gap
- [armel,armhf] properly account for stack randomization and stack guard gap
- [armel,armhf] use STACK\_TOP when computing mmap base address
- block: mq-deadline: Fix queue restart handling
- bpf: fix use after free in prog symbol exposure
- cxgb4: Fix out-of-bounds MSI-X info array access
- erspan: remove the incorrect mtu limit for erspan
- hso: fix NULL-deref on tty open
- ipv6: drop incoming packets having a v4mapped source address
- ipv6: Handle missing host route in \_\_ipv6\_ifa\_notify
- net: ipv4: avoid mixed n\_redirects and rate\_tokens usage
- net: qllogic: Fix memory leak in ql\_alloc\_large\_buffers
- net: Unpublish sk from sk\_reuseport\_cb before call\_rcu
- nfc: fix memory leak in llcp\_sock\_bind()
- qmi\_wwan: add support for Cinterion CLS8 devices
- rxrpc: Fix rxrpc\_recvmmsg tracepoint
- sch\_dsmark: fix potential NULL deref in dsmark\_init()
- udp: fix gso\_segs calculations
- vsock: Fix a lockdep warning in \_\_vsock\_release()
- udp: only do GSO if # of segs > 1
- net/rds: Fix error handling in rds\_ib\_add\_one()
- xen-netfront: do not use ~0U as error return value for xenet\_fill\_frags()
- tipc: fix unlimited bundling of small messages
- sch\_cbq: validate TCA\_CBQ\_WRRROPT to avoid crash
- NFC: fix attrs checks in netlink interface
- kexec: bail out upon SIGKILL when allocating memory.
- 9p/cache.c: Fix memory leak in v9fs\_cache\_session\_get\_cookie

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.79>

- [s390x] process: avoid potential reading of freed stack
- [s390x] KVM: Test for bad access register and size at the start of S390\_MEM\_OP
- [s390x] topology: avoid firing events before kobj are created

- [s390x] cio: exclude subchannels with no parent from pseudo check
- [ppc64el] KVM: Book3S HV: Fix race in re-enabling XIVE escalation interrupts
- [ppc64el] KVM: Book3S HV: Check for MMU ready on piggybacked virtual cores
- [ppc64el] KVM: Book3S HV: Don't lose pending doorbell request on migration on P9
- [x86] KVM: Fix userspace set invalid CR4
- [x86] KVM: nVMX: handle page fault in vmread fix
- nbd: fix max number of supported devs
- PM / devfreq: tegra: Fix kHz to Hz conversion
- ASoC: Define a set of DAPM pre/post-up events
- [armhf] ASoC: sgtl5000: Improve VAG power and mute control
- [ppc64el] mce: Fix MCE handling for huge pages
- [ppc64el] mce: Schedule work from irq\_work
- [ppc64el] powernv: Restrict OPAL symbol map to only be readable by root
- [ppc64el] powernv/ioda: Fix race in TCE level allocation
- [ppc64el] book3s64/mm: Don't do tlbie fixup for some hardware revisions
- tools lib traceevent: Fix "robust" test of do\_generate\_dynamic\_list\_file
- [x86] crypto: qat - Silence smp\_processor\_id() warning
- crypto: skcipher - Unmap pages after an external error
- [mips\*el/loongson-3] Treat Loongson Extensions as ASEs
- power: supply: sbs-battery: use correct flags field
- power: supply: sbs-battery: only return health when battery present
- tracing: Make sure variable reference alias has correct var\_ref\_idx
- usercopy: Avoid HIGHMEM pfn warning
- timer: Read jiffies once when forwarding base clk
- [x86] PCI: vmd: Fix shadow offsets to reflect spec changes
- PCI: Restore Resizable BAR size bits correctly for 1MB BARs
- [armhf] watchdog: imx2\_wdt: fix min() calculation in imx2\_wdt\_set\_timeout
- perf stat: Fix a segmentation fault when using repeat forever
- [armhf] drm/omap: fix max fclk divider for omap36xx
- [arm64] drm/msm/dsi: Fix return value check for clk\_get\_parent
- drm/nouveau/kms/nv50-: Don't create MSTMs for eDP connectors
- [x86] drm/i915/gvt: update vgpu workload head pointer correctly
- mmc: sdhci: improve ADMA error reporting
- Revert "locking/pvqspinlock: Don't wait if vCPU is preempted"
- xen/xenbus: fix self-deadlock after killing user process
- ieee802154: atusb: fix use-after-free at disconnect

- [s390x] cio: avoid calling strlen on null pointer
- cfg80211: initialize on-stack chandefs
- [arm64] cpufeature: Detect SSBS and advertise to userspace
- ima: always return negative code for error
- ima: fix freeing ongoing ahash\_request
- fs: nfs: Fix possible null-pointer dereferences in encode\_attrs()
- 9p: Transport error uninitialized
- 9p: avoid attaching writeback\_fid on mmap with type PRIVATE
- xen/pci: reserve MCFG areas earlier
- ceph: fix directories inode i\_blkbits initialization
- ceph: reconnect connection if session hang in opening state
- watchdog: aspeed: Add support for AST2600
- netfilter: nf\_tables: allow lookups in dynamic sets
- drm/amdgpu: Fix KFD-related kernel oops on Hawaii
- drm/amdgpu: Check for valid number of registers to read
- pNFS: Ensure we do clear the return-on-close layout stateid on fatal errors
- [x86] purgatory: Disable the stackleak GCC plugin for the purgatory
- ntb: point to right memory window index
- thermal: Fix use-after-free when unregistering thermal zone device
- thermal\_hwmon: Sanitize thermal\_zone type
- libnvdimm/region: Initialize bad block for volatile namespaces
- fuse: fix memleak in cuse\_channel\_open
- libnvdimm/nfit\_test: Fix acpi\_handle redefinition
- sched/membarrier: Call sync\_core only before usermode for same mm
- sched/membarrier: Fix private expedited registration check
- sched/core: Fix migration to invalid CPU in \_\_set\_cpus\_allowed\_ptr()
- kernel/elfcore.c: include proper prototypes
- nfp: flower: fix memory leak in nfp\_flower\_spawn\_vnic\_reprs
- drm/radeon: Bail earlier when **radeon.cik** /si\_support=0 is passed
- [ppc64el] KVM: HV: XIVE: Free escalation interrupts before disabling the VP
- [x86] KVM: nVMX: Fix consistency check on injected exception error code
- nbd: fix crash when the blksize is zero
- [ppc64el] pseries: Fix cpu\_hotplug\_lock acquisition in resize\_hpt()
- [ppc64el] radix: Rename CPU\_FTR\_P9\_TLBIE\_BUG feature flag
- tools lib traceevent: Do not free tep->cmdlines in add\_new\_comm() on failure
- tick: broadcast-hrtimer: Fix a race in bc\_set\_next

- perf tools: Fix segfault in `cpu_cache_level__read()`
- perf stat: Reset previous counts on repeat with interval
- [arm64] ssbd: Add support for PSTATE.SSBS rather than trapping to EL3
- [arm64] KVM: Set SCTL\_EL2.DSSBS if SSBD is forcefully disabled and !vhe
- [arm64] docs: Document SSBS HWCAP
- [arm64] fix SSBS sanitization
- [arm64] Add sysfs vulnerability show for spectre-v1
- [arm64] add sysfs vulnerability show for meltdown
- [arm64] enable generic CPU vulnerabilities support
- [arm64] Always enable ssb vulnerability detection
- [arm64] Provide a command line to disable spectre\_v2 mitigation
- [arm64] Advertise mitigation of Spectre-v2, or lack thereof
- [arm64] Always enable spectre-v2 vulnerability detection
- [arm64] add sysfs vulnerability show for spectre-v2
- [arm64] add sysfs vulnerability show for speculative store bypass
- [arm64] ssbs: Don't treat CPUs with SSBS as unaffected by SSB
- [arm64] Force SSBS on context switch
- [arm64] Use firmware to detect CPUs that are not affected by Spectre-v2
- [arm64] speculation: Support 'mitigations=' cmdline option
- vfs: Fix EOVERFLOW testing in `put_compat_statfs64`
- cfg80211: add and use strongly typed element iteration macros
- cfg80211: Use const more consistently in `for_each_element` macros
- nl80211: validate beacon head (CVE-2019-16746)

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.80>

- panic: ensure preemption is disabled during `panic()`
- f2fs: use EINVAL for superblock with invalid magic
- USB: rio500: Remove Rio 500 kernel driver
- USB: yurex: Don't retry on unexpected errors
- USB: yurex: fix NULL-derefs on disconnect
- USB: usb-skeleton: fix runtime PM after driver unbind
- USB: usb-skeleton: fix NULL-deref on disconnect
- xhci: Fix false warning message about wrong bounce buffer write length
- xhci: Prevent device initiated U1/U2 link pm if exit latency is too long
- xhci: Check all endpoints for LPM timeout
- xhci: Fix USB 3.1 capability detection on early xHCI 1.1 spec based hosts
- usb: xhci: wait for CNR controller not ready bit in xhci resume

- xhci: Prevent deadlock when xhci adapter breaks during init
- xhci: Increase STS\_SAVE timeout in xhci\_suspend()
- USB: adutux: fix use-after-free on disconnect
- USB: adutux: fix NULL-derefs on disconnect
- USB: adutux: fix use-after-free on release
- USB: iowarrior: fix use-after-free on disconnect
- USB: iowarrior: fix use-after-free on release
- USB: iowarrior: fix use-after-free after driver unbind
- USB: usblp: fix runtime PM after driver unbind
- USB: chaoskey: fix use-after-free on release
- USB: lduusb: fix NULL-derefs on driver unbind
- serial: uartlite: fix exit path null pointer
- USB: serial: keyspan: fix NULL-derefs on open() and write()
- USB: serial: ftdi\_sio: add device IDs for Sienna and Echelon PL-20
- USB: serial: option: add Telit FN980 compositions
- USB: serial: option: add support for Cinterion CLS8 devices
- USB: serial: fix runtime PM after driver unbind
- USB: usblcd: fix I/O after disconnect
- USB: microtek: fix info-leak at probe
- USB: dummy-hcd: fix power budget for SuperSpeed mode
- USB: legousbtower: fix slab info leak at probe
- USB: legousbtower: fix deadlock on disconnect
- USB: legousbtower: fix potential NULL-deref on disconnect
- USB: legousbtower: fix open after failed reset request
- USB: legousbtower: fix use-after-free on release
- [x86] mei: me: add comet point (lake) LP device ids
- [x86] mei: avoid FW version request on Ibex Peak and earlier
- [armhf,arm64] iio: adc: axp288: Override TS pin bias current for some models
- efivar/ssdt: Don't iterate over EFI vars if no SSDT override was specified
- perf llvm: Don't access out-of-scope array
- perf inject jit: Fix JIT\_CODE\_MOVE filename
- blk-wbt: fix performance regression in wbt scale\_up/scale\_down
- CIFS: Gracefully handle QueryInfo errors during open
- CIFS: Force revalidate inode when dentry is stale
- CIFS: Force reval dentry if LOOKUP\_REVAL flag is set
- kernel/sysctl.c: do not override max\_threads provided by userspace

- mm/vmpressure.c: fix a signedness bug in vmpressure\_register\_event()
- gpiolib: don't clear FLAG\_IS\_OUT when emulating open-drain/open-source
- cifs: use cifsInodeInfo->open\_file\_lock while iterating to avoid a panic
- btrfs: fix incorrect updating of log root tree
- btrfs: fix uninitialized ret in ref-verify
- NFS: Fix O\_DIRECT accounting of number of bytes read/written
- [mips\*] elf\_hwcap: Export userspace ASEs
- ACPICA: ACPI 6.3: PPTT add additional fields in Processor Structure Flags
- ACPI/PPTT: Add support for ACPI 6.3 thread flag
- [arm64] topology: Use PPTT to determine if PE is a thread
- vfs: Fix the locking in dcache\_readdir() and friends
- media: stkwebcam: fix runtime PM after driver unbind
- [arm64] sve: Fix wrong free for task->thread.sve\_state
- [rt] tracing/hwlat: Report total time spent in all NMIs during the sample
- [rt] tracing/hwlat: Don't ignore outer-loop duration when calculating max\_latency
- ftrace: Get a reference counter for the trace\_array on filter files
- tracing: Get trace\_array reference for available\_tracers files
- hwmon: Fix HWMON\_P\_MIN\_ALARM mask
- [x86] asm: Fix MWAITX C-state hint value
- [x86] PCI: vmd: Fix config addressing when using bus offsets
- perf/hw\_breakpoint: Fix arch\_hw\_breakpoint use-before-initialization

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.81>

- nvme-pci: Fix a race in controller removal
- scsi: ufs: skip shutdown if hba is not powered
- scsi: megaraid: disable device when probe failed after enabled device
- scsi: qla2xxx: Fix unbound sleep in fcport delete path.
- [armhf] OMAP2+: Fix missing reset done flag for am3 and am43
- [armhf] OMAP2+: Fix warnings with broken omap2\_set\_init\_voltage()
- xen/efi: Set nonblocking callbacks
- nl80211: fix null pointer dereference
- mac80211: fix txq null pointer dereference
- netfilter: nft\_connlimit: disable bh on garbage collection
- [mips\*el/loongson-3] Fix the link time qualifier of 'serial\_exit()'
- [arm64] net: hisilicon: Fix usage of uninitialized variable in function mdio\_sc\_cfg\_reg\_write()
- lib: textsearch: fix escapes in example code
- r8152: Set macpassthru in reset\_resume callback

- libata/ahci: Fix PCS quirk application
- md/raid0: fix warning message for parameter default\_layout
- ocfs2: fix panic due to ocfs2\_wq is null
- ipv4: fix race condition between route lookup and invalidation
- net: avoid potential infinite loop in tc\_ctl\_action()
- net: ipv6: fix listify ip6\_rev\_finish in case of forwarding
- [armhf,arm64] net: stmmac: disable/enable ptp\_ref\_clk in suspend/resume flow
- sctp: change sctp\_prot .no\_autobind with true
- memfd: Fix locking when tagging pins
- USB: legousbtower: fix memleak on disconnect
- ALSA: hda/realtek - Add support for ALC711
- [x86] ALSA: hda/realtek - Enable headset mic on Asus MJ401TA
- ALSA: usb-audio: Disable quirks for BOSS Katana amplifiers
- ALSA: hda - Force runtime PM on Nvidia HDMI codecs
- USB: serial: ti\_usb\_3410\_5052: fix port-close races
- USB: lduusb: fix memleak on disconnect
- USB: usblp: fix use-after-free on disconnect
- USB: lduusb: fix read info leaks
- [mips\*] tbxex: Fix build\_restore\_pagemask KScratch restore
- staging: wlan-ng: fix exit return when sme->key\_idx >= NUM\_WEPKEYS
- [s390x] scsi: zfcp: fix reaction on bit error threshold notification
- scsi: sd: Ignore a failure to sync cache due to lack of authorization
- scsi: core: save/restore command resid for error handling
- scsi: core: try to get module before removing device
- scsi: ch: Make it possible to open a ch device multiple times again
- Input: synaptics-rmi4 - avoid processing unknown IRQs
- ACPI: CPPC: Set pcc\_data[pcc\_ss\_id] to NULL in acpi\_cppc\_processor\_exit()
- cfg80211: wext: avoid copying malformed SSIDs (CVE-2019-17133)
- mac80211: Reject malformed SSID elements
- [x86] drm/edid: Add 6 bpc quirk for SDC panel in Lenovo G50
- drm/ttm: Restore ttm prefaulting
- drm/amdgpu: Bail earlier when **amdgpu.cik**/si\_support is not set to 1
- drivers/base/memory.c: don't access uninitialized memmaps in soft\_offline\_page\_store()
- fs/proc/page.c: don't access uninitialized memmaps in fs/proc/page.c
- mm/memory-failure.c: don't access uninitialized memmaps in memory\_failure()
- mm/slub: fix a deadlock in show\_slab\_objects()

- mm/page\_owner: don't access uninitialized memmaps when reading /proc/pagetypeinfo
- hugetlbf: don't access uninitialized memmaps in pfn\_range\_valid\_gigantic()
- mm/memory-failure: poison read receives SIGKILL instead of SIGBUS if mmaped more than once
- EDAC/ghes: Fix Use after free in ghes\_edac remove path
- [arm64] Enable workaround for Cavium TX2 erratum 219 when running SMT
- CIFS: avoid using MID 0xFFFF
- CIFS: Fix use after free of file info structures
- perf/aux: Fix AUX output stopping
- tracing: Fix race in perf\_trace\_buf initialization
- dm cache: fix bugs when a GFP\_NOWAIT allocation fails
- [amd64] boot: Make level2\_kernel\_pgt pages invalid outside kernel area
- [x86] apic/x2apic: Fix a NULL pointer deref when handling a dying cpu
- [x86] pinctrl: cherryview: restore Strago DMI workaround for all versions
- [arm64] pinctrl: armada-37xx: fix control of pins 32 and up
- [arm64] pinctrl: armada-37xx: swap polarity on LED group
- btrfs: block-group: Fix a memory leak due to missing btrfs\_put\_block\_group()
- Btrfs: add missing extents release on file extent cluster relocation error
- Btrfs: check for the full sync flag while holding the inode lock during fsync
- btrfs: tracepoints: Fix bad entry members of qgroup events
- memstick: jmb38x\_ms: Fix an error handling path in 'jmb38x\_ms\_probe()'
- cpufreq: Avoid cpufreq\_suspend() deadlock on system shutdown
- xen/netback: fix error path of xenlif\_connect\_data()
- PCI: PM: Fix pci\_power\_up()
- blk-rq-qos: fix first node deletion of rq\_qos\_del()
- RDMA/cxgb4: Do not dma memory off of the stack (CVE-2019-17075)

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.82>

- zram: fix race between backing\_dev\_show and backing\_dev\_store
- dm snapshot: introduce account\_start\_copy() and account\_end\_copy()
- dm snapshot: rework COW throttling to fix deadlock
- Btrfs: fix inode cache block reserve leak on failure to allocate data space
- Btrfs: fix memory leak due to concurrent append writes with fiemap
- btrfs: qgroup: Always free PREALLOC META reserve in btrfs\_delalloc\_release\_extents()
- btrfs: tracepoints: Fix wrong parameter order for qgroup events
- wil6210: fix freeing of rx buffers in EDMA mode
- f2fs: flush quota blocks after turning it off
- scsi: lpfc: Fix a duplicate 0711 log message number.



- f2fs: fix to recover inode's i\_gc\_failures during POR
- f2fs: fix to recover inode->i\_flags of inode block during POR
- [x86] HID: i2c-hid: add Direkt-Tek DTLAPY133-1 to descriptor override
- [arm64,armel,armhf] usb: dwc2: fix unbalanced use of external vbus-supply
- [x86] tools/power turbostat: fix goldmont C-state limit decoding
- [x86] cpu: Add Atom Tremont (Jacobsville)
- [arm64] drm/msm/dpu: handle failures while initializing displays
- bcache: fix input overflow to writeback\_rate\_minimum
- PCI: Fix Switchtec DMA aliasing quirk dmesg noise
- Btrfs: fix deadlock on tree root leaf when finding free extent
- netfilter: ipset: Make invalid MAC address checks consistent
- HID: i2c-hid: Disable runtime PM for LG touchscreen
- HID: i2c-hid: Ignore input report if there's no data present on Elan touchpanels
- HID: i2c-hid: Add Odys Winbook 13 to descriptor override
- [x86] platform/x86: Add the VLV ISP PCI ID to atomisp2\_pm
- [x86] platform/x86: Fix config space access for intel\_atomisp2\_pm
- ath10k: assign 'n\_cipher\_suites = 11' for WCN3990 to enable WPA3
- HID: Add ASUS T100CHI keyboard dock battery quirks
- NFSv4: Ensure that the state manager exits the loop on SIGKILL
- HID: steam: fix boot loop with bluetooth firmware
- HID: steam: fix deadlock with input devices.
- [arm64,armhf] usb: dwc3: gadget: early giveback if End Transfer already completed
- [arm64,armhf] usb: dwc3: gadget: clear DWC3\_EP\_TRANSFER\_STARTED on cmd complete
- ALSA: usb-audio: Cleanup DSD whitelist
- usb: handle warm-reset port requests on hub resume
- [armhf] rtc: pcf8523: set xtal load capacitance from DT
- [arm64] Add MIDR encoding for HiSilicon Taishan CPUs
- [arm64] kpti: Whitelist HiSilicon Taishan v110 CPUs
- scsi: lpfc: Correct localport timeout duration error
- CIFS: Respect SMB2 hdr preamble size in read responses
- cifs: add credits from unmatched responses/messages
- ALSA: hda/realtek - Apply ALC294 hp init also for S4 resume
- ext4: disallow files with EXT4\_JOURNAL\_DATA\_FL from EXT4\_IOC\_SWAP\_BOOT
- exec: load\_script: Do not exec truncated interpreter path
- [arm64,armhf] net: dsa: mv88e6xxx: Release lock while requesting IRQ
- PCI/PME: Fix possible use-after-free on remove

- [arm64,armhf] iio: adc: meson\_saradc: Fix memory allocation order
- [x86] iio: fix center temperature of bmc150-accel-core
- perf map: Fix overlapped map handling
- perf script brstackinsn: Fix recovery from LBR/binary mismatch
- perf jevents: Fix period for Intel fixed counters
- perf tools: Propagate get\_cpuid() error
- perf annotate: Propagate perf\_env\_\_arch() error
- perf annotate: Fix the signedness of failure returns
- perf annotate: Propagate the symbol\_\_annotate() error return
- perf annotate: Return appropriate error code for allocation failures
- staging: rtl8188eu: fix null dereference when kzalloc fails
- RDMA/hfi1: Prevent memory leak in sdma\_init (CVE-2019-19065)
- RDMA/iwcm: Fix a lock inversion issue
- [x86] HID: hyperv: Use in-place iterator API in the channel callback
- nfs: Fix nfsi->nrequests count error on nfs\_inode\_remove\_request
- [arm64] ftrace: Ensure synchronisation in PLT setup for Neoverse-N1
- [arm64] gpio: max77620: Use correct unit for debounce times
- fs: cifs: mute -Wunused-const-variable message
- [armhf] serial: mctrl\_gpio: Check for NULL pointer
- efi/cper: Fix endianness of PCIe class code
- [x86] efi/x86: Do not clean dummy variable in kexec path
- [x86] xen: Return from panic notifier
- ocfs2: clear zero in unaligned direct IO
- fs: ocfs2: fix possible null-pointer dereferences in ocfs2\_xa\_prepare\_entry()
- fs: ocfs2: fix a possible null-pointer dereference in ocfs2\_write\_end\_nolock()
- fs: ocfs2: fix a possible null-pointer dereference in ocfs2\_info\_scan\_inode\_alloc()
- [arm64] armv8\_deprecated: Checking return value for memory allocation
- [x86] cpu: Add Comet Lake to the Intel CPU models header
- sched/vtime: Fix guest/system mis-accounting on task switch
- [x86] perf/x86/amd: Change/fix NMI latency mitigation to use a timestamp
- drm/amdgpu: fix memory leak
- iio: imu: adis16400: release allocated memory on failure (CVE-2019-19060)
- [x86] virt: vbox: fix memory leak in hgcm\_call\_preprocess\_linaddr (CVE-2019-19048)
- NFSv4: Fix leak of clp->cl\_acceptor string
- tracing: Initialize iter->seq after zeroing in tracing\_read\_pipe()
- ALSA: hda/realtek: Reduce the Headphone static noise on XPS 9350/9360

- iwlwifi: exclude GEO SAR support for 3168
- nbd: verify socket is supported during setup
- USB: legousbtower: fix a signedness bug in tower\_probe()
- [x86] thunderbolt: Use 32-bit writes when writing ring producer/consumer
- ath6kl: fix a NULL-ptr-deref bug in ath6kl\_usb\_alloc\_urb\_from\_pipe() (CVE-2019-15098)
- fuse: flush dirty data/metadata before non-truncate setattr
- fuse: truncate pending writes on O\_TRUNC
- ALSA: bebob: Fix prototype of helper function to return negative value
- ALSA: hda/realtek - Fix 2 front mics of codec 0x623
- ALSA: hda/realtek - Add support for ALC623
- UAS: Revert commit 3ae62a42090f (“UAS: fix alignment of scatter/gather segments”)
- USB: gadget: Reject endpoints with 0 maxpacket value
- usb-storage: Revert commit 747668dbc061 (“usb-storage: Set virt\_boundary\_mask to avoid SG overflows”)
- USB: lduusb: fix ring-buffer locking
- USB: lduusb: fix control-message timeout
- usb: xhci: fix \_\_le32/\_\_le64 accessors in debugfs code
- USB: serial: whiteheat: fix potential slab corruption
- USB: serial: whiteheat: fix line-speed endianness
- scsi: target: cxgbit: Fix cxgbit\_fw4\_ack()
- HID: i2c-hid: add Trekstor Primebook C11B to descriptor override
- HID: Fix assumption that devices have inputs
- HID: fix error message in hid\_open\_report()
- nl80211: fix validation of mesh path nexthop
- [s390x] cmm: fix information leak in cmm\_timeout\_handler()
- [s390x] idle: fix cpu idle time calculation
- [arm64] Ensure VM\_WRITE|VM\_SHARED ptes are clean by default
- rtlwifi: Fix potential overflow on P2P code (CVE-2019-17666)
- [arm64] dmaengine: qcom: bam\_dma: Fix resource leak
- [armhf] dmaengine: cppi41: Fix cppi41\_dma\_prep\_slave\_sg() when idle
- NFS: Fix an RCU lock leak in nfs4\_refresh\_delegation\_stateid()
- batman-adv: Avoid free/alloc race when handling OGM buffer
- llc: fix sk\_buff leak in llc\_sap\_state\_process()
- llc: fix sk\_buff leak in llc\_conn\_service()
- rxrpc: Fix call ref leak
- rxrpc: rxrpc\_peer needs to hold a ref on the rxrpc\_local record

- rxrpc: Fix trace-after-put looking at the put peer record
- NFC: pn533: fix use-after-free and memleaks
- bonding: fix potential NULL deref in bond\_update\_slave\_arr
- net: usb: sr9800: fix uninitialized local variable
- sch\_netem: fix rcu splat in netem\_enqueue()
- ALSA: timer: Simplify error path in snd\_timer\_open()
- ALSA: timer: Fix mutex deadlock at releasing card
- ALSA: usb-audio: DSD auto-detection for Playback Designs
- ALSA: usb-audio: Update DSD support quirks for Oppo and Rotel
- ALSA: usb-audio: Add DSD support for Gustard U16/X26 USB Interface
- [ppc64el] powerpc/powernv: Fix CPU idle to be called with IRQs disabled
- Revert "ALSA: hda: Flush interrupts on disabling"

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.83>

- regulator: of: fix suspend-min/max-voltage parsing
- [arm64] dts: allwinner: a64: pine64-plus: Add PHY regulator delay
- [arm64] arm64: dts: allwinner: a64: sopine-baseboard: Add PHY regulator delay
- [armhf] regulator: ti-abb: Fix timeout in ti\_abb\_wait\_txdone/ti\_abb\_clear\_all\_txdone
- [x86] ASoC: rt5682: add NULL handler to set\_jack function
- [armhf] regulator: pfuze100-regulator: Variable "val" in pfuze100\_regulator\_probe() could be uninitialized
- [arm64,armhf] ASoc: rockchip: i2s: Fix RPM imbalance
- [armel,armhf] mm: fix alignment handler faults under memory pressure
- scsi: qla2xxx: fix a potential NULL pointer dereference
- scsi: scsi\_dh\_alua: handle RTPG sense code correctly during state transitions
- drm/amdgpu: fix potential VM faults
- scsi: target: core: Do not overwrite CDB byte 1
- tracing: Fix "gfp\_t" format for synthetic events
- of: unittest: fix memory leak in unittest\_data\_add (CVE-2019-19049)
- [arm64,armhf] irqchip/gic-v3-its: Use the exact ITSList for VMOVP
- cifs: Fix cifsInodeInfo lock\_sem deadlock when reconnect occurs
- nbd: protect cmd->status with cmd->lock
- nbd: handle racing with error'ed out commands
- cxgb4: fix panic when attaching to ULD fail
- dccp: do not leak jiffies on the wire
- erspan: fix the tun\_info options\_len check for erspan
- inet: stop leaking jiffies on the wire

- net: annotate accesses to sk->sk\_incoming\_cpu
- net: annotate lockless accesses to sk->sk\_napi\_id
- [armhf] net: dsa: bcm\_sf2: Fix IMP setup for port different than 8
- net: fix sk\_page\_frag() recursion from memory reclaim
- [arm64] net: hisilicon: Fix ping latency when deal with high throughput
- net/mlx4\_core: Dynamically set guaranteed amount of counters per VF
- netns: fix GFP flags in rtnl\_net\_notifyid()
- net: usb: lan78xx: Disable interrupts before calling generic\_handle\_irq()
- net: Zeroing the structure ethtool\_wolinfo in ethtool\_get\_wol()
- udp: fix data-race in udp\_set\_dev\_scratch()
- vxlan: check tun\_info options\_len properly
- net: add skb\_queue\_empty\_lockless()
- udp: use skb\_queue\_empty\_lockless()
- net: use skb\_queue\_empty\_lockless() in poll() handlers
- net: use skb\_queue\_empty\_lockless() in busy poll contexts
- net: add READ\_ONCE() annotation in \_\_skb\_wait\_for\_more\_packets()
- ipv4: fix route update on metric change.
- net/mlx5e: Fix handling of compressed CQEs in case of low NAPI budget
- r8169: fix wrong PHY ID issue with RTL8168dp
- net/mlx5e: Fix ethtool self test: link speed
- [armhf] net: dsa: b53: Do not clear existing mirrored port mask
- [armhf] net: phy: bcm7xxx: define soft\_reset for 40nm EPHY
- net: usb: lan78xx: Connect PHY before registering MAC
- [arm64,armhf] net: dsa: fix switch tree list
- r8152: add device id for Lenovo ThinkPad USB-C Dock Gen 2
- net/flow\_dissector: switch to siphash
- wireless: Skip directory when generating certificates
- [x86] platform/x86: pmc\_atom: Add Siemens SIMATIC IPC227E to critclk\_systems DMI table
- [ppc64el] powerpc/mm: Fixup tlbie vs mtpidr/mtlpidr ordering issue on POWER9
- usb: gadget: udc: core: Fix segfault if udc\_bind\_to\_driver() for pending driver fails

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.84>

- bonding: fix state transition issue in link monitoring
- CDC-NCM: handle incomplete transfer of MTU
- ipv4: Fix table id reference in fib\_sync\_down\_addr
- [mips\*] net: ethernet: octeon\_mgmt: Account for second possible VLAN header
- net: fix data-race in neigh\_event\_send()

- net: usb: qmi\_wwan: add support for DW5821e with eSIM support
- nfc: netlink: fix double device reference drop
- qede: fix NULL pointer deref in \_\_qede\_remove()
- ipv6: fixes rt6\_probe() and fib6\_nh->last\_probe init
- [arm64] net: hns: Fix the stray netpoll locks causing deadlock in NAPI path
- ALSA: timer: Fix incorrectly assigned timer instance
- ALSA: bebob: fix to detect configured source of sampling clock for Focusrite Saffire Pro i/o series
- ALSA: hda/ca0132 - Fix possible workqueue stall
- mm: memcontrol: fix network errors from failing \_\_GFP\_ATOMIC charges
- mm, meminit: recalculate pcpu batch and high limits after init completes
- mm: thp: handle page cache THP correctly in PageTransCompoundMap
- mm, vmstat: hide /proc/pagetypeinfo from normal users
- dump\_stack: avoid the livelock of the dump\_lock
- perf tools: Fix time sorting
- drm/radeon: fix si\_enable\_smc\_cac() failed issue
- HID: wacom: generic: Treat serial number and related fields as unsigned
- [arm64] Do not mask out PTE\_RDONLY in pte\_same()
- ceph: fix use-after-free in \_\_ceph\_remove\_cap()
- ceph: add missing check in d\_revalidate snapdir handling
- [armhf] sunxi: Fix CPU powerdown on A83T
- netfilter: nf\_tables: Align nft\_expr private data to 64-bit
- netfilter: ipset: Fix an error code in ip\_set\_sockfn\_get()
- [x86] intel\_th: pci: Add Comet Lake PCH support
- [x86] intel\_th: pci: Add Jasper Lake PCH support
- [x86] apic/32: Avoid bogus LDR warnings
- SMB3: Fix persistent handles reconnect
- can: usb\_8dev: fix use-after-free on disconnect
- [armhf] can: flexcan: disable completely the ECC mechanism
- can: peak\_usb: fix a potential out-of-sync while decoding packets
- can: rx-offload: can\_rx\_offload\_queue\_sorted(): fix error handling, avoid skb mem leak
- can: gs\_usb: gs\_can\_open(): prevent memory leak (CVE-2019-19052)
- can: dev: add missing of\_node\_put() after calling of\_get\_child\_by\_name()
- can: mcba\_usb: fix use-after-free on disconnect
- can: peak\_usb: fix slab info leak
- configfs: stash the data we need into configfs\_buffer at open time
- configfs\_register\_group() shouldn't be (and isn't) called in rmdirable parts

- configs: new object representing tree fragments
- configs: provide exclusion between IO and removals
- configs: fix a deadlock in configs\_symlink()
- ALSA: usb-audio: More validations of descriptor units
- ALSA: usb-audio: Simplify parse\_audio\_unit()
- ALSA: usb-audio: Unify the release of usb\_mixer\_elem\_info objects
- ALSA: usb-audio: Remove superfluous bLength checks
- ALSA: usb-audio: Clean up check\_input\_term()
- ALSA: usb-audio: Fix possible NULL dereference at create\_yamaha\_midi\_quirk()
- ALSA: usb-audio: remove some dead code
- ALSA: usb-audio: Fix copy&paste error in the validator
- sched/fair: Fix low cpu usage with high throttling by removing expiration of cpu-local slices
- sched/fair: Fix -Wunused-but-set-variable warnings
- usbip: Fix vhci\_urb\_enqueue() URB null transfer buffer error path
- usbip: Implement SG support to vhci-hcd and stub driver
- [arm64,armhf] PCI: tegra: Enable Relaxed Ordering only for Tegra20 & Tegra30
- [amd64] HID: intel-ish-hid: fix wrong error handling in ishtp\_cl\_alloc\_tx\_ring()
- RDMA/mlx5: Clear old rate limit when closing QP
- iw\_cxgb4: fix ECN check on the passive accept
- RDMA/qedr: Fix reported firmware version
- net/mlx5e: TX, Fix consumer index of error cq dump
- net/mlx5: prevent memory leak in mlx5\_fpga\_conn\_create\_cq (CVE-2019-19045)
- scsi: qla2xxx: fixup incorrect usage of host\_byte
- RDMA/uverbs: Prevent potential underflow
- net: openvswitch: free vport unless register\_netdevice() succeeds
- scsi: lpfc: Honor module parameter lpfc\_use\_adisc
- scsi: qla2xxx: Initialized mailbox to prevent driver load failure
- netfilter: nf\_flow\_table: set timeout before insertion into hashes
- ipvs: don't ignore errors in case refcounting ip\_vs module fails
- ipvs: move old\_secure\_tcp into struct netns\_ipvs
- bonding: fix unexpected IFF\_BONDING bit unset
- macsec: fix refcnt leak in module exit routine
- usb: gadget: composite: Fix possible double free memory bug
- [arm64] usb: dwc3: pci: prevent memory leak in dwc3\_pci\_probe (CVE-2019-18813)
- usb: gadget: configs: fix concurrent issue between composite APIs
- [arm64,armhf] usb: dwc3: remove the call trace of USBx\_GFLADJ

- [x86] perf/x86/amd/ibs: Fix reading of the IBS OpData register and thus precise RIP validity
  - [x86] perf/x86/amd/ibs: Handle erratum #420 only on the affected CPU family (10h)
  - [x86] perf/x86/uncore: Fix event group support
  - USB: Skip endpoints with 0 maxpacket length
  - USB: lusb: use unsigned size format specifiers
  - usbip: tools: Fix read\_usb\_vudc\_device() error path handling
  - RDMA/iw\_cxgb4: Avoid freeing skb twice in arp failure case
  - [arm64] RDMA/hns: Prevent memory leaks of eq->buf\_list
  - scsi: qla2xxx: stop timer in shutdown path
  - nvme-multipath: fix possible io hang after ctrl reconnect
  - [amd64] fjes: Handle workqueue allocation failure
  - [arm64] net: hisilicon: Fix "Trying to free already-free IRQ"
  - drm/amdgpu: If amdgpu\_ib\_schedule fails return back the error.
  - [x86] hv\_netvsc: Fix error handling in netvsc\_attach()
  - [arm64,armhf] usb: dwc3: gadget: fix race when disabling ep with cancelled xfers
  - NFSv4: Don't allow a cached open with a revoked delegation
  - igb: Fix constant media auto sense switching when no cable is connected
  - e1000: fix memory leaks
  - [x86] pinctrl: intel: Avoid potential glitches if pin is in GPIO mode
  - ocfs2: protect extent tree in ocfs2\_prepare\_inode\_for\_write()
  - [x86] pinctrl: cherryview: Fix irq\_valid\_mask calculation
  - blkcg: make blkcg\_print\_stat() print stats only for online blkgs
  - [x86] iio: imu: mpu6050: Add support for the ICM 20602 IMU
  - [x86] iio: imu: inv\_mpu6050: fix no data on MPU6050
  - mm/filemap.c: don't initiate writeback if mapping has no dirty pages
  - cgroup,writeback: don't switch wbs immediately on dead wbs if the memcg is dead
  - usbip: Fix free of unallocated memory in vhci tx
  - netfilter: ipset: Copy the right MAC address in hash:ip,mac IPv6 sets
  - net: prevent load/store tearing on sk->sk\_stamp
  - [x86] iio: imu: mpu6050: Fix FIFO layout for ICM20602
  - vsock/virtio: fix sock refcnt holding during the shutdown
  - x86/cpu: Add Tremont to the cpu vulnerability whitelist
- <https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.85>
- scsi: core: Handle drivers which set sg\_tablesize to zero
  - ax88172a: fix information leak on short answers
  - ipmr: Fix skb headroom in ipmr\_get\_route().



- net: gemini: add missed free\_netdev
- net: usb: qmi\_wwan: add support for Foxconn T77W968 LTE modules
- slip: Fix memory leak in slip\_open error path
- ALSA: usb-audio: Fix missing error check at mixer resolution test
- ALSA: usb-audio: not submit urb for stopped endpoint
- ALSA: usb-audio: Fix incorrect NULL check in create\_yamaha\_midi\_quirk()
- ALSA: usb-audio: Fix incorrect size check for processing/extension units
- Btrfs: fix log context list corruption after rename exchange operation
- Input: ff-memless - kill timer in destroy()
- Input: synaptics-rmi4 - fix video buffer size
- Input: synaptics-rmi4 - disable the relative position IRQ in the F12 driver
- Input: synaptics-rmi4 - do not consume more data than we have (F11, F12)
- Input: synaptics-rmi4 - clear IRQ enables for F54
- Input: synaptics-rmi4 - destroy F54 poller workqueue when removing
- IB/hfi1: Ensure full Gen3 speed in a Gen4 system
- IB/hfi1: Use a common pad buffer for 9B and 16B packets
- i2c: acpi: Force bus speed to 400KHz if a Silead touchscreen is present
- ecryptfs\_lookup\_interpose(): lower\_dentry->d\_inode is not stable
- ecryptfs\_lookup\_interpose(): lower\_dentry->d\_parent is not stable either
- [armhf] net: ethernet: dwmac-sun8i: Use the correct function in exit path
- [x86] iommu/vt-d: Fix QI\_DEV\_IOTLB\_PFSID and QI\_DEV\_EIOTLB\_PFSID macros
- mm: mempolicy: fix the wrong return value and potential pages leak of mbind
- mm: memcg: switch to css\_tryget() in get\_mem\_cgroup\_from\_mm()
- mm: hugetlb: switch to css\_tryget() in hugetlb\_cgroup\_charge\_cgroup()
- iio: adc: max9611: explicitly cast gain\_selectors
- tee: optee: take DT status property into account
- ath10k: fix kernel panic by moving pci flush after napi\_disable
- clk: sunxi-ng: h6: fix PWM gate/reset offset
- soundwire: Initialize completion for defer messages
- [x86] soundwire: intel: Fix uninitialized adev deref
- [arm64] dts: allwinner: a64: Orange Pi Win: Fix SD card node
- [arm64] dts: allwinner: a64: Olinuxino: fix DRAM voltage
- [arm64] dts: allwinner: a64: NanoPi-A64: Fix DCDC1 voltage
- ALSA: pcm: signedness bug in snd\_pcm\_plug\_alloc()
- [arm64] soc/tegra: pmc: Fix pad voltage configuration for Tegra186
- [arm64] dts: tegra210-p2180: Correct sdmmc4 vqmmc-supply

- y2038: make do\_gettimeofday() and get\_seconds() inline
- rtc: sysfs: fix NULL check in rtc\_add\_groups()
- remoteproc/davinci: Use %zx for formatting size\_t
- extcon: cht-wc: Return from default case to avoid warnings
- cfg80211: Avoid regulatory restore when COUNTRY\_IE\_IGNORE is set
- ALSA: seq: Do error checks at creating system ports
- ath10k: skip resetting rx filter for WCN3990
- ath9k: fix tx99 with monitor mode interface
- wil6210: drop Rx multicast packets that are looped-back to STA
- wil6210: set edma variables only for Talyn-MB devices
- wil6210: prevent usage of tx ring 0 for eDMA
- wil6210: fix invalid memory access for rx\_buff\_mgmt debugfs
- ath10k: limit available channels via DT ieee80211-freq-limit
- ice: Update request resource command to latest specification
- ice: Prevent control queue operations during reset
- gfs2: Don't set GFS2\_RDF\_UPTODATE when the lvb is updated
- ice: Fix and update driver version string
- ASoC: dapm: Don't fail creating new DAPM control on NULL pinctrl
- ASoC: dpcm: Properly initialise hw->rate\_max
- ASoC: meson: axg-fifo: report interrupt request failure
- ASoC: AMD: Change MCLK to 48Mhz
- pinctrl: ingenic: Probe driver at subsys\_initcall
- [armhf] dts: exynos: Use i2c-gpio for HDMI-DDC on Arndale
- [armhf] dts: exynos: Fix HDMI-HPD line handling on Arndale
- [armhf] dts: exynos: Fix sound in Snow-rev5 Chromebook
- liquidio: fix race condition in instruction completion processing
- [arm64] dts: stratix10: i2c clock running out of spec
- [armhf] dts: exynos: Fix regulators configuration on Peach Pi/Pit Chromebooks
- i40evf: Validate the number of queues a PF sends
- i40e: use correct length for strncpy
- i40evf: set IFF\_UNICAST\_FLT flag for the VF
- i40e: Check and correct speed values for link on open
- i40evf: Don't enable vlan stripping when rx offload is turned on
- i40e: hold the rtnl lock on clearing interrupt scheme
- i40evf: cancel workqueue sync for adminq when a VF is removed
- i40e: Prevent deleting MAC address from VF when set by PF

- IB/rxe: avoid back-to-back retries
- IB/rxe: fixes for rdma read retry
- iwlfwif: drop packets with bad status in CD
- iwlfwif: don't WARN on trying to dump dead firmware
- iwlfwif: mvm: avoid sending too many BARS
- media: vicodec: fix out-of-range values when decoding
- media: i2c: Fix pm\_runtime\_get\_if\_in\_use() usage in sensor drivers
- media: ov772x: Disable clk on error path
- rtl8187: Fix warning generated when strncpy() destination length matches the size argument
- mwifex: do no submit URB in suspended state
- mwifex: free rx\_cmd skb in suspended state
- brcmfmac: fix wrong strncpy usage
- mt76: Fix comparisons with invalid hardware key index
- soc: imx: gpc: fix PDN delay
- ASoC: rsnd: ssi: Fix issue in dma data address assignment
- net: hns3: Fix for multicast failure
- net: hns3: Fix error of checking used vlan id
- net: hns3: Fix for loopback selftest failed problem
- net: hns3: Change the dst mac addr of loopback packet
- net/mlx5: Fix atomic\_mode enum values
- net: phy: mscc: read 'vsc8531,vddmac' as an u32
- net: phy: mscc: read 'vsc8531, edge-slowdown' as an u32
- [armhf] dts: meson8: fix the clock controller register size
- [armhf] dts: meson8b: fix the clock controller register size
- mtd: rawnand: marvell: use regmap\_update\_bits() for syscon access
- mtd: rawnand: fsl\_ifc: check result of SRAM initialization
- mtd: rawnand: fsl\_ifc: fixup SRAM init for newer ctrl versions
- mtd: rawnand: qcom: don't include dma-direct.h
- IB/mlx5: Change TX affinity assignment in RoCE LAG mode
- qxl: fix null-pointer crash during suspend
- mac80211: fix saving a few HE values
- cfg80211: validate wmm rule when setting
- f2fs: avoid wrong decrypted data from disk
- net: lan78xx: Bail out if lan78xx\_get\_endpoints fails
- rtnetlink: move type calculation out of loop
- ASoC: sgtl5000: avoid division by zero if lo\_vag is zero

- ath10k: avoid possible memory access violation
- [armhf] dts: exynos: Disable pull control for S5M8767 PMIC
- ath10k: wmi: disable softirq's while calling ieee80211\_rx
- i2c: mediatek: Use DMA safe buffers for i2c transactions
- IB/mlx5: Don't hold spin lock while checking device state
- IB/ipoib: Ensure that MTU isn't less than minimum permitted
- RDMA/core: Rate limit MAD error messages
- RDMA/core: Follow correct unregister order between sysfs and cgroup
- udf: Fix crash during mount
- ASoC: dapm: Avoid uninitialised variable warning
- [x86] ASoC: Intel: hdac\_hdmi: Limit sampling rates at dai creation
- ata: Disable AHCI ALPM feature for Ampere Computing eMAG SATA
- [powerpc] make PowerMac cache node search conditional on CONFIG\_PPC\_PMAC
- [armhf] dts: omap3-gta04: give spi\_lcd node a label so that we can overwrite in other DTS files
- [armhf] dts: omap3-gta04: fixes for tvout / venc
- [armhf] dts: omap3-gta04: tvout: enable as display1 alias
- [armhf] dts: omap3-gta04: fix touchscreen tsc2007
- [armhf] dts: omap3-gta04: make NAND partitions compatible with recent U-Boot
- [armhf] dts: omap3-gta04: keep vpll2 always on
- f2fs: submit bio after shutdown
- failover: Fix error return code in net\_failover\_create
- sched/debug: Explicitly cast sched\_feat() to bool
- sched/debug: Use symbolic names for task state constants
- firmware: arm\_scmi: use strcpy to ensure NULL-terminated strings
- [arm64] dts: rockchip: Fix VCC5V0\_HOST\_EN on rk3399-sapphire
- [armhf] dts: exynos: Disable pull control for PMIC IRQ line on Artik5 board
- usb: mtu3: disable vbus rise/fall interrupts of ltssm
- EDAC, sb\_edac: Return early on ADDR\_V bit and address type test
- [armhf] rtc: pl030: fix possible race condition
- ath9k: add back support for using active monitor interfaces for tx99
- dmaengine: at\_xdma: remove a stray bottom half unlock
- RDMA/hns: Fix an error code in hns\_roce\_v2\_init\_eq\_table()
- IB/hfi1: Missing return value in error path for user sdma
- signal: Always ignore SIGKILL and SIGSTOP sent to the global init
- signal: Properly deliver SIGILL from uprobes
- signal: Properly deliver SIGSEGV from x86 uprobes

- f2fs: fix memory leak of write\_io in fill\_super()
- f2fs: fix memory leak of percpu counter in fill\_super()
- f2fs: fix setattr project check upon fssetattr ioctl
- scsi: qla2xxx: Use correct qpair for ABTS/CMD
- scsi: qla2xxx: Fix iDMA error
- scsi: qla2xxx: Defer chip reset until target mode is enabled
- scsi: qla2xxx: Terminate Plogi/PRLI if WWN is 0
- scsi: qla2xxx: Fix deadlock between ATIO and HW lock
- scsi: qla2xxx: Increase abort timeout value
- scsi: qla2xxx: Check for Register disconnect
- scsi: qla2xxx: Fix port speed display on chip reset
- scsi: qla2xxx: Fix dropped srb resource.
- scsi: qla2xxx: Fix duplicate switch's Nport ID entries
- scsi: lpfc: Fix GFT\_ID and PRLI logic for RSCN
- scsi: lpfc: Correct invalid EQ doorbell write on if\_type=6
- scsi: lpfc: Fix errors in log messages.
- scsi: sym53c8xx: fix NULL pointer dereference panic in sym\_int\_sir()
- [armhf] imx6: register pm\_power\_off handler if "fsl,pmic-stby-poweroff" is set
- scsi: pm80xx: Corrected dma\_unmap\_sg() parameter
- scsi: pm80xx: Fixed system hang issue during kexec boot
- kprobes: Don't call BUG\_ON() if there is a kprobe in use on free list
- net: aquantia: fix hw\_atl\_utils\_fw\_upload\_dwords
- Drivers: hv: vmbus: Fix synic per-cpu context initialization
- nvme: core: return error code instead of NULL from nvme\_device\_get
- media: dt-bindings: adv748x: Fix decimal unit addresses
- [x86] ALSA: hda: Fix implicit definition of pci\_iomap() on SH
- media: fix: media: pci: meye: validate offset to avoid arbitrary access
- media: dvb: fix compat ioctl translation
- net: bcmgenet: Fix speed selection for reverse MII
- [arm64] dts: meson: libretech: update board model
- [arm64] dts: meson-axg: use the proper compatible for ethmac
- [x86] ALSA: intel8x0m: Register irq handler after register initializations
- [arm64] dts: renesas: salvator-common: adv748x: Override secondary addresses
- [arm64] dts: renesas: r8a77965: Attach the SYS-DMAC to the IPMMU
- [arm64] dts: renesas: r8a77965: Fix HS-USB compatible
- [arm64] dts: renesas: r8a77965: Fix clock/reset for usb2\_phy1

- pinctrl: at91-pio4: fix has\_config check in atmel\_pctl\_dt\_subnode\_to\_map()
- llc: avoid blocking in llc\_sap\_close()
- [armhf] dts: qcom: ipq4019: fix cpu0's qcom,saw2 reg value
- [arm64] soc: qcom: wcnss\_ctrl: Avoid string overflow
- [arm64] dts: broadcom: Fix I2C and SPI bus warnings
- [armhf] dts: bcm: Fix SPI bus warnings
- [armhf] dts: aspeed: Fix I2C bus warnings
- [ppc64el,powerpc\*] powerpc/vdso: Correct call frame information
- [armhf] dts: socfpga: Fix I2C bus unit-address error
- [armhf] dts: sunxi: Fix I2C bus warnings
- [armhf] dts: sun9i: Fix I2C bus warnings
- android: binder: no outgoing transaction when thread todo has transaction
- cxgb4: Fix endianness issue in t4\_fwcache()
- [arm64] fix for bad\_mode() handler to always result in panic
- block, bfq: inject other-queue I/O into seeky idle queues on NCQ flash
- blok, bfq: do not plug I/O if all queues are weight-raised
- [arm64] dts: meson: Fix erroneous SPI bus warnings
- power: supply: ab8500\_fg: silence uninitialized variable warnings
- component: fix loop condition to call unbind() if bind() fails
- kernfs: Fix range checks in kernfs\_get\_target\_path
- ip\_gre: fix parsing gre header in ipgre\_err
- scsi: ufshcd: Fix NULL pointer dereference for in ufshcd\_init
- [armhf] dts: rockchip: Fix erroneous SPI bus dtc warnings on rk3036
- [arm64] dts: rockchip: Fix I2C bus unit-address error on rk3399-puma-haikou
- [x86] ACPI / LPSS: Exclude I2C busses shared with PUNIT from pmc\_atom\_d3\_mask
- netfilter: nf\_tables: avoid BUG\_ON usage
- ath9k: Fix a locking bug in ath9k\_add\_interface()
- [s390x] qeth: uninstall IRQ handler on device removal
- [s390x] qeth: invoke softirqs after napi\_schedule()
- media: vsp1: Fix vsp1\_regs.h license header
- media: vsp1: Fix YCbCr planar formats pitch calculation
- media: ov2680: don't register the v4l2 subdevice before checking chip ID
- PCI/ACPI: Correct error message for ASPM disabling
- net: socionext: Fix two sleep-in-atomic-context bugs in ave\_rxfifo\_reset()
- PCI: mediatek: Fix unchecked return value
- [armhf] dts: xilinx: Fix I2C and SPI bus warnings

- serial: uartps: Fix suspend functionality
- serial: samsung: Enable baud clock for UART reset procedure in resume
- serial: mxs-auart: Fix potential infinite loop
- tty: serial: qcom\_geni\_serial: Fix serial when not used as console
- [arm64] dts: ti: k3-am65: Change #address-cells and #size-cells of interconnect to 2
- samples/bpf: fix a compilation failure
- spi: mediatek: Don't modify spi\_transfer when transfer.
- ASoC: rt5682: Fix the boost volume at the beginning of playback
- ipmi\_si\_pci: fix NULL device in ipmi\_si error message
- ipmi\_si: fix potential integer overflow on large shift
- ipmi:dmi: Ignore IPMI SMBIOS entries with a zero base address
- ipmi: fix return value of ipmi\_set\_my\_LUN
- net: hns3: fix return type of ndo\_start\_xmit function
- net: cavium: fix return type of ndo\_start\_xmit function
- net: ibm: fix return type of ndo\_start\_xmit function
- [ppc64el,powerpc\*] iommu: Avoid dereference before pointer check
- [ppc64el,powerpc\*] selftests: Do not fail with reschedule
- [ppc64el,powerpc64] hash: Fix stab\_rr off by one initialization
- [ppc64el,powerpc64] pseries/memory-hotplug: Only update DT once per memory DLPAR request
- [ppc64el,powerpc64] pseries: Disable CPU hotplug across migrations
- [ppc64el,powerpc\*] Fix duplicate const clang warning in user access code
- RDMA/i40iw: Fix incorrect iterator type
- OPP: Protect dev\_list with opp\_table lock
- of/unittest: Fix I2C bus unit-address error
- libfdt: Ensure INT\_MAX is defined in libfdt\_env.h
- power: supply: twl4030\_charger: fix charging current out-of-bounds
- power: supply: twl4030\_charger: disable eoc interrupt on linear charge
- net: mvpp2: fix the number of queues per cpu for PPv2.2
- net: marvell: fix return type of ndo\_start\_xmit function
- net: toshiba: fix return type of ndo\_start\_xmit function
- net: xilinx: fix return type of ndo\_start\_xmit function
- net: broadcom: fix return type of ndo\_start\_xmit function
- net: amd: fix return type of ndo\_start\_xmit function
- net: sun: fix return type of ndo\_start\_xmit function
- net: hns3: Fix for setting speed for phy failed problem
- net: hns3: Fix cmdq registers initialization issue for vf

- net: hns3: Clear client pointer when initialize client failed or uninitialize finished
- net: hns3: Fix client initialize state issue when roce client initialize failed
- net: hns3: Fix parameter type for q\_id in hclge\_tm\_q\_to\_qs\_map\_cfg()
- nfp: provide a better warning when ring allocation fails
- usb: chipidea: imx: enable OTG overcurrent in case USB subsystem is already started
- usb: chipidea: Fix otg event handler
- usb: usbtmc: Fix ioctl USBTMC\_IOCTL\_ABORT\_BULK\_OUT
- [s390x] zcrypt: enable AP bus scan without a valid default domain
- [s390x] vdso: avoid 64-bit vdso mapping for compat tasks
- [s390x] vdso: correct CFI annotations of vDSO functions
- brcmfmac: increase buffer for obtaining firmware capabilities
- brcmsmac: Use kvmalloc() for ucode allocations
- mlxsw: spectrum: Init shaper for TCs 8..15
- PCI: portdrv: Initialize service drivers directly
- [armhf] dts: am335x-evm: fix number of cpsw
- [armhf] dts: ti: Fix SPI and I2C bus warnings
- f2fs: avoid infinite loop in f2fs\_alloc\_nid
- f2fs: fix to recover inode's uid/gid during POR
- [armhf] dts: ux500: Correct SCU unit address
- [armhf] dts: ux500: Fix LCDA clock line muxing
- [armhf] dts: ste: Fix SPI controller node names
- spi: pic32: Use proper enum in dmaengine\_prep\_slave\_rg
- crypto: chacha20 - Fix chacha20\_block() keystream alignment (again)
- cpufeature: avoid warning when compiling with clang
- [armhf] crypto: crc32 - avoid warning when compiling with Clang
- [armel] dts: marvell: Fix SPI and I2C bus warnings
- [x86] mce-inject: Reset injection struct after injection
- [armhf,arm64] dts: clearfog: fix sdhci supply property name
- bnx2x: Ignore bandwidth attention in single function mode
- PCI/AER: Take reference on error devices
- PCI/AER: Don't read upstream ports below fatal errors
- PCI/ERR: Use slot reset if available
- samples/bpf: fix compilation failure
- net: phy: mdio-bcm-unimac: Allow configuring MDIO clock divider
- net: micrel: fix return type of ndo\_start\_xmit function
- net: freescale: fix return type of ndo\_start\_xmit function



- [x86] CPU: Use correct macros for Cyrix calls
- [x86] CPU: Change query logic so CPUID is enabled before testing
- EDAC: Correct DIMM capacity unit symbol
- [mips\*] kexec: Relax memory restriction
- [arm64] dts: rockchip: Fix microSD in rk3399 sapphire board
- mlxsw: Make MLXSW\_SP1\_FWREV\_MINOR a hard requirement
- media: imx: work around false-positive warning, again
- media: pci: ivtv: Fix a sleep-in-atomic-context bug in ivtv\_yuv\_init()
- media: au0828: Fix incorrect error messages
- media: davinci: Fix implicit enum conversion warning
- [armhf] dts: rockchip: explicitly set vcc\_sd0 pin to gpio on rk3188-radxa-rock
- usb: gadget: uvc: configs: Drop leaked references to config items
- usb: gadget: uvc: configs: Prevent format changes after linking header
- usb: gadget: uvc: configs: Sort frame intervals upon writing
- [armhf] dts: exynos: Correct audio subsystem parent clock on Peach Chromebooks
- i2c: aspeed: fix invalid clock parameters for very large divisors
- gpiolib: Fix gpio\_direction\_\* for single direction GPIOs
- phy: brcm-sata: allow PHY\_BRCM\_SATA driver to be built for DSL SoCs
- phy: renesas: rcar-gen3-usb2: fix vbus\_ctrl for role sysfs
- phy: phy-twl4030-usb: fix denied runtime access
- [armhf] dts: imx6ull: update vdd\_soc voltage for 900MHz operating point
- usb: gadget: uvc: Factor out video USB request queuing
- usb: gadget: uvc: Only halt video streaming endpoint in bulk mode
- coresight: Use ERR\_CAST instead of ERR\_PTR
- coresight: Fix handling of sinks
- coresight: perf: Fix per cpu path management
- coresight: perf: Disable trace path upon source error
- coresight: tmc-etr: Handle driver mode specific ETR buffers
- coresight: etm4x: Configure EL2 exception level when kernel is running in HYP
- coresight: tmc: Fix byte-address alignment for RRP
- coresight: dynamic-replicator: Handle multiple connections
- slimbus: ngd: register ngd driver only once.
- slimbus: ngd: return proper error code instead of zero
- slimbus: ngd: register controller after power up.
- misc: kgdbts: Fix restrict error
- misc: genwqe: should return proper error value.

- vmbus: keep pointer to ring buffer page
- vfio/pci: Fix potential memory leak in vfio\_msi\_cap\_len
- vfio/pci: Mask buggy SR-IOV VF INTx support
- iw\_cxgb4: Use proper enumerated type in c4iw\_bar2\_addrs
- scsi: libsas: always unregister the old device if going to discover new
- f2fs: fix remount problem of option io\_bits
- phy: lantiq: Fix compile warning
- [arm64] dts: fsl: Fix I2C and SPI bus warnings
- [armhf] dts: imx51-zii-rdu1: Fix the rtc compatible string
- [arm64] tegra: I2C on Tegra194 is not compatible with Tegra114
- [armhf] dts: tegra30: fix xcvr-setup-use-fuses
- [armhf] dts: tegra20: restore address order
- [armhf] tegra: apalis\_t30: fix mmc1 cmd pull-up
- [armhf] tegra: apalis\_t30: fix mcp2515 can controller interrupt polarity
- [armhf] tegra: colibri\_t30: fix mcp2515 can controller interrupt polarity
- [armhf] dts: paz00: fix wakeup gpio keycode
- net: smsc: fix return type of ndo\_start\_xmit function
- net: faraday: fix return type of ndo\_start\_xmit function
- PCI/ERR: Run error recovery callbacks for all affected devices
- f2fs: update i\_size after DIO completion
- f2fs: fix to recover inode's project id during POR
- f2fs: mark inode dirty explicitly in recover\_inode()
- RDMA: Fix dependencies for rdma\_user\_mmap\_io
- EDAC: Raise the maximum number of memory controllers
- firmware: dell\_rbu: Make payload memory uncachable
- Bluetooth: hci\_serdev: clear HCI\_UART\_PROTO\_READY to avoid closing proto races
- Bluetooth: L2CAP: Detect if remote is not able to use the whole MPS
- Bluetooth: btrsi: fix bt tx timeout issue
- [x86] hyperv: Suppress "PCI: Fatal: No config space access function found"
- crypto: s5p-sss: Fix race in error handling
- crypto: s5p-sss: Fix Fix argument list alignment
- crypto: fix a memory leak in rsa-kcs1pad's encryption mode
- iwlfwifi: dbg: don't crash if the firmware crashes in the middle of a debug dump
- iwlfwifi: fix non\_shared\_ant for 22000 devices
- iwlfwifi: pcie: read correct prph address for newer devices
- iwlfwifi: api: annotate compressed BA notif array sizes

- iwlfwif: pcie: gen2: build A-MSDU only for GSO
- iwlfwif: pcie: fit reclaim msg to MAX\_MSG\_LEN
- iwlfwif: mvm: use correct FIFO length
- iwlfwif: mvm: Allow TKIP for AP mode
- scsi: NCR5380: Clear all unissued commands on host reset
- scsi: NCR5380: Have NCR5380\_select() return a bool
- scsi: NCR5380: Withhold disconnect privilege for REQUEST SENSE
- scsi: NCR5380: Use DRIVER\_SENSE to indicate valid sense data
- scsi: NCR5380: Check for invalid reselection target
- scsi: NCR5380: Don't clear busy flag when abort fails
- scsi: NCR5380: Don't call dsprintk() following reselection interrupt
- scsi: NCR5380: Handle BUS FREE during reselection
- scsi: NCR5380: Check for bus reset
- [arm64] dts: amd: Fix SPI bus warnings
- [arm64] dts: lg: Fix SPI controller node names
- rtc: isl1208: avoid possible sysfs race
- rtc: tx4939: fixup nvmmem name and register size
- rtc: armada38x: fix possible race condition
- netfilter: masquerade: don't flush all conntracks if only one address deleted on device
- usb: xhci-mtk: fix ISOC error when interval is zero
- usb: usbtmc: uninitialized symbol 'actual' in usbtmc\_ioctl\_clear
- fuse: use READ\_ONCE on congestion\_threshold and max\_background
- IB/iser: Fix possible NULL deref at iser\_inv\_desc()
- media: ov2680: fix null dereference at power on
- [s390x] vdso: correct vdso mapping for compat tasks
- net: phy: mdio-bcm-unimac: mark PM functions as \_\_maybe\_unused
- memfd: Use radix\_tree\_deref\_slot\_protected to avoid the warning.
- slcan: Fix memory leak in error path

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.86>

- spi: mediatek: use correct mata->xfer\_len when in fifo transfer
- i2c: mediatek: modify threshold passed to i2c\_get\_dma\_safe\_msg\_buf()
- tee: optee: add missing of\_node\_put after of\_device\_is\_available
- Revert "OPP: Protect dev\_list with opp\_table lock"
- net: cdc\_ncm: Signedness bug in cdc\_ncm\_set\_dgram\_size()
- idr: Fix idr\_get\_next race with idr\_remove
- mm/memory\_hotplug: don't access uninitialized memmaps in shrink\_pgdat\_span()

- mm/memory\_hotplug: fix updating the node span
- [arm64] uaccess: Ensure PAN is re-enabled after unhandled uaccess fault
- fbdev: Ditch fb\_edid\_add\_monspecs
- [i386] bpf, x32: Fix bug for BPF\_ALU64 | BPF\_NEG
- [i386] bpf, x32: Fix bug with ALU64 {LSH, RSH, ARSH} BPF\_X shift by 0
- [i386] bpf, x32: Fix bug with ALU64 {LSH, RSH, ARSH} BPF\_K shift by 0
- [i386] bpf, x32: Fix bug for BPF\_JMP | {BPF\_JSGT, BPF\_JSLE, BPF\_JSLT, BPF\_JSGE}
- net: ovs: fix return type of ndo\_start\_xmit function
- net: xen-netback: fix return type of ndo\_start\_xmit function
- [armhf] dts: dra7: Enable workaround for errata i870 in PCIe host mode
- [armhf] dts: omap5: enable OTG role for DWC3 controller
- [arm64] net: hns3: Fix for netdev not up problem when setting mtu
- [arm64] net: hns3: Fix loss of coal configuration while doing reset
- f2fs: return correct errno in f2fs\_gc
- [armhf] dts: sun8i: h3-h5: ir register size should be the whole memory block
- [armhf] dts: sun8i: h3: bpi-m2-plus: Fix address for external RGMII Ethernet PHY
- tcp: up initial rmem to 128KB and SYN rwin to around 64KB
- SUNRPC: Fix priority queue fairness
- ACPI / LPSS: Make acpi\_lpss\_find\_device() also find PCI devices
- ACPI / LPSS: Resume BYT/CHT I2C controllers from resume\_noirq
- f2fs: keep lazytime on remount
- IB/hfi1: Error path MAD response size is incorrect
- IB/hfi1: Ensure ucast\_dlid access doesnt exceed bounds
- mt76x2: fix tx power configuration for VHT mcs 9
- mt76x2: disable WLAN core before probe
- mt76: fix handling ps-poll frames
- [arm64,armhf] iommu/io-pgtable-arm: Fix race handling in split\_blk\_unmap()
- [arm64,armhf] iommu/arm-smmu-v3: Fix unexpected CMD\_SYNC timeout
- [arm64,armhf] kvm: Fix stage2\_flush\_memslot for 4 level page table
- [arm64] numa: Report correct memblock range for the dummy node
- ath10k: fix vdev-start timeout on error
- rtlwifi: btcoex: Use proper enumerated types for Wi-Fi only interface
- ata: ahci\_brcm: Allow using driver or DSL SoCs
- PM / devfreq: Fix devfreq\_add\_device() when drivers are built as modules.
- PM / devfreq: Fix handling of min/max\_freq == 0
- PM / devfreq: stopping the governor before device\_unregister()

- ath9k: fix reporting calculated new FFT upper max
- selftests/tls: Fix recv(MSG\_PEEK) & splice() test cases
- usb: gadget: udc: fotg210-udc: Fix a sleep-in-atomic-context bug in fotg210\_get\_status()
- usb: dwc3: gadget: Check ENBLSLPM before sending ep command
- nl80211: Fix a GET\_KEY reply attribute
- [arm64,armhf] irqchip/irq-mvebu-icu: Fix wrong private data retrieval
- watchdog: core: fix null pointer dereference when releasing cdev
- watchdog: w83627hf\_wdt: Support NCT6796D, NCT6797D, NCT6798D
- [ppc64el,powerpc64] Inform the userspace about TCE update failures
- printk: Do not miss new messages when replaying the log
- printk: CON\_PRINTBUFFER console registration is a bit racy
- dmaengine: ep93xx: Return proper enum in ep93xx\_dma\_chan\_direction
- dmaengine: timb\_dma: Use proper enum in td\_prep\_slave\_sg
- [x86] ALSA: hda: Fix mismatch for register mask and value in ext controller.
- ext4: fix build error when DX\_DEBUG is defined
- clk: keystone: Enable TISCI clocks if K3\_ARCH
- sunrpc: Fix connect metrics
- [x86] PCI: Apply VMD's AERSID fixup generically
- mei: samples: fix a signedness bug in amt\_host\_if\_call()
- cxgb4: Use proper enum in cxgb4\_dcb\_handle\_fw\_update
- cxgb4: Use proper enum in IEEE\_FAUX\_SYNC
- [ppc64el,powerpc\*] Fix DTL buffer registration
- [ppc64el,powerpc\*] Fix how we iterate over the DTL entries
- [ppc64el,powerpc\*] xive: Move a dereference below a NULL test
- mtd: rawnand: sh\_fctl: Use proper enum for fctl\_dma\_fifo0\_transfer
- PM / hibernate: Check the success of generating md5 digest before hibernation
- tools: PCI: Fix compilation warnings
- ice: Fix forward to queue group logic
- md: allow metadata updates while suspending an array - fix
- ixgbe: Fix ixgbe TX hangs with XDP\_TX beyond queue limit
- i40e: Use proper enum in i40e\_ndo\_set\_vf\_link\_state
- ixgbe: Fix crash with VFs and flow director on interface flap
- IB/mthca: Fix error return code in \_\_mthca\_init\_one()
- IB/rxe: avoid srq memory leak
- RDMA/hns: Bugfix for reserved qp number
- RDMA/hns: Submit bad wr when post send wr exception

- RDMA/hns: Bugfix for CM test
- RDMA/hns: Limit the size of extend sge of sq
- IB/mlx4: Avoid implicit enumerated type conversion
- rpmsg: glink: smem: Support rx peak for size less than 4 bytes
- msm/gpu/a6xx: Force of\_dma\_configure to setup DMA for GMU
- OPP: Return error on error from dev\_pm\_opp\_get\_opp\_count()
- ACPIA: Never run \_REG on system\_memory and system\_IO
- cpuidle: menu: Fix wakeup statistics updates for polling state
- ASoC: qdsp6: q6asm-dai: checking NULL vs IS\_ERR()
- [ppc64el,powerpc\*] time: Use clockevents\_register\_device(), fixing an issue with large decremter
- [ppc64el,powerpc64] radix: Explicitly flush ERAT with local LPID invalidation
- ata: ep93xx: Use proper enums for directions
- qed: Avoid implicit enum conversion in qed\_ooo\_submit\_tx\_buffers
- media: rc: ir-rc6-decoder: enable toggle bit for Kathrein RCU-676 remote
- media: pxa\_camera: Fix check for pdev->dev.of\_node
- media: rcar-vin: fix redeclaration of symbol
- media: i2c: adv748x: Support probing a single output
- [x86] ALSA: hda/sigmatel - Disable automute for Elo VuPoint
- bnxt\_en: return proper error when FW returns HWRM\_ERR\_CODE\_RESOURCE\_ACCESS\_DENIED
- [ppc64el,powerpc64] Book3S PR: Exiting split hack mode needs to fixup both PC and LR
- USB: serial: cypress\_m8: fix interrupt-out transfer length
- usb: dwc2: disable power\_down on rockchip devices
- mtd: physmap\_of: Release resources on error
- cpu/SMT: State SMT is disabled even with nosmt and without “=force”
- brcmfmac: reduce timeout for action frame scan
- brcmfmac: fix full timeout waiting for action frame on-channel tx
- qtnfmac: request userspace to do OBSS scanning if FW can not
- qtnfmac: pass sgi rate info flag to wireless core
- qtnfmac: inform wireless core about supported extended capabilities
- qtnfmac: drop error reports for out-of-bounds key indexes
- [armhf] clk: samsung: Use NOIRQ stage for Exynos5433 clocks suspend/resume
- [armhf] clk: samsung: exynos5420: Define CLK\_SECKEY gate clock only or Exynos5420
- [armhf] clk: samsung: Use clk\_hw API for calling clk framework from clk notifiers
- printk: Correct wrong casting
- NFSv4.x: fix lock recovery during delegation recall
- dmaengine: ioat: fix prototype of ioat\_enumerate\_channels

- media: ov5640: fix framerate update
- media: cec-gpio: select correct Signal Free Time
- gfs2: slow the deluge of io error messages
- i2c: omap: use core to detect 'no zero length' quirk
- i2c: qup: use core to detect 'no zero length' quirk
- i2c: tegra: use core to detect 'no zero length' quirk
- i2c: zx2967: use core to detect 'no zero length' quirk
- Input: st1232 - set INPUT\_PROP\_DIRECT property
- Input: silead - try firmware reload after unsuccessful resume
- soc: fsl: bman\_portals: defer probe after bman's probe
- net: hns3: Fix for rx vlan id handle to support Rev 0x21 hardware
- tc-testing: fix build of eBPF programs
- remoteproc: Check for NULL firmwares in sysfs interface
- remoteproc: qcom: q6v5: Fix a race condition on fatal crash
- kexec: Allocate decrypted control pages for kdump if SME is enabled
- [x86] olpc: Fix build error with CONFIG\_MFD\_CS5535=m
- dmaengine: rcar-dmac: set scatter/gather max segment size
- xfrm: use correct size to initialise sp->ovec
- ACPI / SBS: Fix rare oops when removing modules
- iwlfwif: mvm: don't send keys when entering D3
- xsk: proper AF\_XDP socket teardown ordering
- [amd64] fsgsbase: Fix ptrace() to read the FS/GS base accurately
- mmc: renesas\_sdhi\_internal\_dmac: Whitelist r8a774a1
- mmc: tmio: Fix SCC error detection
- mmc: renesas\_sdhi\_internal\_dmac: set scatter/gather max segment size
- fbdev: sbuslib: use checked version of put\_user()
- fbdev: sbuslib: integer overflow in sbusfb\_ioctl\_helper()
- fbdev: fix broken menu dependencies
- reset: Fix potential use-after-free in \_\_of\_reset\_control\_get()
- bcache: account size of buckets used in uuid write to ca->meta\_sectors\_written
- bcache: recal cached\_dev\_sectors on detach
- [x86] platform: mlx-platform: Properly use mlxplat\_mlxcpld\_msn201x\_items
- media: dw9714: Fix error handling in probe function
- media: dw9807-vcn: Fix probe error handling
- media: cx18: Don't check for address of video\_dev
- mtd: spi-nor: cadence-quadspi: Use proper enum for dma\_[un]map\_single

- mtd: devices: m25p80: Make sure WRITE\_EN is issued before each write
- [x86] intel\_rdt: Introduce utility to obtain CDP peer
- [x86] intel\_rdt: CBM overlap should also check for overlap with CDP peer
- mmc: mmci: expand startbiterr to irqmask and error check
- [s390x] kasan: avoid vdso instrumentation
- [s390x] kasan: avoid instrumentation of early C code
- [s390x] kasan: avoid user access code instrumentation
- [i386] proc/vmcore: Fix i386 build error of missing copy\_oldmem\_page\_encrypted()
- backlight: lm3639: Unconditionally call led\_classdev\_unregister
- mfd: ti\_am335x\_tscadc: Keep ADC interface on if child is wakeup capable
- printk: Give error on attempt to set log buffer length to over 2G
- media: isif: fix a NULL pointer dereference bug
- GFS2: Flush the GFS2 delete workqueue before stopping the kernel threads
- media: cx231xx: fix potential sign-extension overflow on large shift
- media: venus: vdec: fix decoded data size
- [x86] ALSA: hda/ca0132 - Fix input effect controls for desktop cards
- lightnvm: pblk: fix rqd.error return value in pblk\_blk\_erase\_sync
- lightnvm: pblk: fix incorrect min\_write\_pgs
- lightnvm: pblk: guarantee emeta on line close
- lightnvm: pblk: fix write amplification calculation
- lightnvm: pblk: guarantee mw\_cunits on read buffer
- lightnvm: do no update csecs and sos on 1.2
- lightnvm: pblk: fix error handling of pblk\_lines\_init()
- lightnvm: pblk: consider max hw sectors supported for max\_write\_pgs
- [x86] kexec: Correct KEXEC\_BACKUP\_SRC\_END off-by-one error
- bpf: btf: Fix a missing check bug
- net: fix generic XDP to handle if eth header was mangled
- gpio: syscon: Fix possible NULL ptr usage
- spi: fsl-lpspi: Prevent FIFO under/overflow by default
- pinctrl: gemini: Mask and set properly
- spi: spidev: Fix OF tree warning logic
- [armel,armhf] 8802/1: Call syscall\_trace\_exit even when system call skipped
- [x86] mm: Do not warn about PCI BIOS W+X mappings
- orangefs: rate limit the client not running info message
- pinctrl: gemini: Fix up TVC clock group
- scsi: arcmsr: clean up clang warning on extraneous parentheses



- [x86] hwmon: (k10temp) Support all Family 15h Model 6xh and Model 7xh processors
- hwmon: (nct6775) Fix names of DIMM temperature sources
- hwmon: (pwm-fan) Silence error on probe deferral
- hwmon: (ina3221) Fix INA3221\_CONFIG\_MODE macros
- hwmon: (npcm-750-pwm-fan) Change initial pwm target to 255
- selftests: forwarding: Have lldpad\_app\_wait\_set() wait for unknown, too
- net: sched: avoid writing on noop\_qdisc
- netfilter: nft\_compat: do not dump private area
- misc: cxl: Fix possible null pointer dereference
- mac80211: minstrel: fix using short preamble CCK rates on HT clients
- mac80211: minstrel: fix CCK rate group streams value
- mac80211: minstrel: fix sampling/reporting of CCK rates in HT mode
- spi: rockchip: initialize dma\_slave\_config properly
- mlxsw: spectrum\_switchdev: Check notification relevance based on upper device
- [armhf] dts: omap5: Fix dual-role mode on Super-Speed port
- tcp: start receiver buffer autotuning sooner
- ACPI / LPSS: Use acpi\_lpss\_\* instead of acpi\_subsys\_\* functions for hibernate
- PM / devfreq: Fix static checker warning in try\_then\_request\_governor
- tools: PCI: Fix broken pcitest compilation
- [ppc64el,powerpc\*] time: Fix clockevent\_decrementer initialisation for PR KVM
- mmc: tmio: fix SCC error handling to avoid false positive CRC error
- [x86] resctrl: Fix rdt\_find\_domain() return value and checks

<https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.87>

- mlxsw: spectrum\_router: Fix determining underlay for a GRE tunnel
- net/mlx4\_en: fix mlx4 ethtool -N insertion
- net/mlx4\_en: Fix wrong limitation for number of TX rings
- net: rtnetlink: prevent underflows in do\_setvinfo()
- net/sched: act\_pedit: fix WARN() in the traffic path
- net: sched: ensure opts\_len <= IP\_TUNNEL\_OPTS\_MAX in act\_tunnel\_key
- sfc: Only cancel the PPS workqueue if it exists
- net/mlx5e: Fix set vf link state error flow
- net/mlxfw: Verify FSM error code translation doesn't exceed array size
- net/mlx5: Fix auto group size calculation
- vhost/vsock: split packets to send using multiple buffers
- gpio: max77620: Fixup debounce delays
- tools: gpio: Correctly add make dependencies for gpio\_utils

- nbd:fix memory leak in nbd\_get\_socket()
- virtio\_console: allocate inbufs in add\_port() only if it is needed
- Revert "fs: ocfs2: fix possible null-pointer dereferences in ocfs2\_xa\_prepare\_entry()"
- mm/ksm.c: don't WARN if page is still mapped in remove\_stable\_node()
- [x86] drm/amd/powerplay: issue no PPSMC\_MSG\_GetCurrPkgPwr on unsupported ASICs
- [x86] drm/i915/pmu: "Frequency" is reported as accumulated cycles
- [x86] drm/i915/userptr: Try to acquire the page lock around set\_page\_dirty()
- mwifiex: Fix NL80211\_TX\_POWER\_LIMITED
- ALSA: isight: fix leak of reference to firewire unit in error path of .probe callback
- crypto: testmgr - fix sizeof() on COMP\_BUF\_SIZE
- printk: lock/unlock console only for new logbuf entries
- printk: fix integer overflow in setup\_log\_buf()
- pinctrl: madera: Fix uninitialized variable bug in madera\_mux\_set\_mux
- PCI: cadence: Write MSI data with 32bits
- gfs2: Fix marking bitmaps non-full
- pty: fix compat ioctls
- synclink\_gt(): fix compat\_ioctl()
- [ppc64] Fix signedness bug in update\_flash\_db()
- [powerpc] boot: Fix opal console in boot wrapper
- [ppc64\*,powerpc] boot: Disable vector instructions
- [ppc64\*,powerpc] eeh: Fix null deref for devices removed during EEH
- [ppc64\*,powerpc] eeh: Fix use of EEH\_PE\_KEEP on wrong field
- EDAC, thunderx: Fix memory leak in thunderx\_l2c\_threaded\_isr()
- mt76: do not store aggregation sequence number for null-data frames
- mt76x0: phy: fix restore phase in mt76x0\_phy\_recalibrate\_after\_assoc
- brcmsmac: AP mode: update beacon when TIM changes
- ath10k: set probe request oui during driver start
- ath10k: allocate small size dma memory in ath10k\_pci\_diag\_write\_mem
- skd: fixup usage of legacy IO API
- cdrom: don't attempt to fiddle with cdo->capability
- spi: sh-msiof: fix deferred probing
- mmc: mediatek: fill the actual clock for mmc debugfs
- mmc: mediatek: fix cannot receive new request when msdc\_cmd\_is\_ready fail
- PCI: mediatek: Fix class type for MT7622 to PCI\_CLASS\_BRIDGE\_PCI
- btrfs: defrag: use btrfs\_mod\_outstanding\_extents in cluster\_pages\_for\_defrag
- btrfs: handle error of get\_old\_root

- gsmi: Fix bug in append\_to\_eventlog sysfs handler
- misc: mic: fix a DMA pool free failure
- w1: IAD Register is yet readable trough iad sys file. Fix sprintf (%u for unsigned, count for max size).
- [m68k] fix command-line parsing when passed from u-boot
- RDMA/bnxt\_re: Avoid NULL check after accessing the pointer
- RDMA/bnxt\_re: Fix qp async event reporting
- RDMA/bnxt\_re: Avoid resource leak in case the NQ registration fails
- pinctrl: sunxi: Fix a memory leak in 'sunxi\_pinctrl\_build\_state()'
- pwm: lpss: Only set update bit if we are actually changing the settings
- amiflop: clean up on errors during setup
- qed: Align local and global PTT to propagate through the APIs.
- scsi: ips: fix missing break in switch
- nfp: bpf: protect against mis-initializing atomic counters
- [x86] KVM: nVMX: reset cache/shadows when switching loaded VMCS
- [x86] KVM: nVMX: move check\_vmentry\_postreqs() call to nested\_vmx\_enter\_non\_root\_mode()
- [x86] KVM: Fix invvpid and invept register operand size in 64-bit mode
- clk: tegra: Fixes for MBIST work around
- scsi: isci: Use proper enumerated type in atapi\_d2h\_reg\_frame\_handler
- scsi: isci: Change sci\_controller\_start\_task's return type to sci\_status
- scsi: bfa: Avoid implicit enum conversion in bfa\_im\_post\_vendor\_event
- scsi: iscsi\_tcp: Explicitly cast param in iscsi\_sw\_tcp\_host\_get\_param
- nvmet: avoid integer overflow in the discard code
- nvmet-fcloop: suppress a compiler warning
- nvme-pci: fix hot removal during error handling
- PCI: mediatek: Fixup MSI enablement logic by enabling MSI before clocks
- clk: mmp2: fix the clock id for sdh2\_clk and sdh3\_clk
- ASoC: tegra\_sgtl5000: fix device\_node refcounting
- scsi: dc395x: fix dma API usage in srb\_done
- scsi: dc395x: fix DMA API usage in sg\_update\_list
- scsi: zorro\_esp: Limit DMA transfers to 65535 bytes
- net: dsa: mv88e6xxx: Fix 88E6141/6341 2500mbps SERDES speed
- net: fix warning in af\_unix
- xfs: fix use-after-free race in xfs\_buf\_rele
- xfs: clear ail delwri queued bufs on unmount of shutdown fs
- kprobes, x86/ptrace.h: Make regs\_get\_kernel\_stack\_nth() not fault on bad stack
- ACPI / scan: Create platform device for INT33FE ACPI nodes

- PM / Domains: Deal with multiple states but no governor in genpd
- ALSA: i2c/cs8427: Fix int to char conversion
- macintosh/windfarm\_smu\_sat: Fix debug output
- PCI: vmd: Detach resources after stopping root bus
- USB: misc: appledisplay: fix backlight update\_status return code
- usbip: tools: fix atoi() on non-null terminated string
- sctp: use sk\_wmem\_queued to check for writable space
- dm raid: avoid bitmap with raid4/5/6 journal device
- selftests/bpf: fix file resource leak in load\_kallsyms
- SUNRPC: Fix a compile warning for cmpxchg64()
- sunrpc: safely reallocate resvport min/max inversion
- atm: zatm: Fix empty body Clang warnings
- [s390x] perf: Return error when debug\_register fails
- swiotlb: do not panic on mapping failures
- spi: omap2-mcspi: Set FIFO DMA trigger level to word length
- [x86] intel\_rdt: Prevent pseudo-locking from using stale pointers
- sparc: Fix parport build warnings.
- [ppc64\*,powerpc] pseries: Export raw per-CPU VPA data via debugfs
- [ppc64\*,powerpc] mm/radix: Fix off-by-one in split mapping logic
- [ppc64\*,powerpc] mm/radix: Fix overuse of small pages in splitting logic
- [ppc64\*,powerpc] mm/radix: Fix small page at boundary when splitting
- [ppc64\*] radix: Fix radix\_\_flush\_tlb\_collapsed\_pmd double flushing pmd
- selftests/bpf: fix return value comparison for tests in test\_libbpf.sh
- tools: bpftool: fix completion for "bpftool map update"
- ceph: fix dentry leak in ceph\_readdir\_prepopulate
- ceph: only allow punch hole mode in fallocate
- thermal: armada: fix a test in probe()
- f2fs: fix to spread clear\_cold\_data()
- f2fs: spread f2fs\_set\_inode\_flags()
- mISDN: Fix type of switch control variable in ctrl\_teimanager
- qlcnic: fix a return in qlcnic\_dcb\_get\_capability()
- net: ethernet: ti: cpsw: unsync mcast entries while switch promisc mode
- mfd: arizona: Correct calling of runtime\_put\_sync
- mfd: mc13xxx-core: Fix PMIC shutdown when reading ADC values
- [x86] mfd: intel\_soc\_pmic\_bxtwc: Chain power button IRQs as well
- mfd: max8997: Enable irq-wakeup unconditionally

- net: socionext: Stop PHY before resetting netsec
- fs/cifs: fix uninitialised variable warnings
- spi: uniphier: fix incorrect property items
- selftests/ftrace: Fix to test kprobe \$comm arg only if available
- selftests: watchdog: fix message when /dev/watchdog open fails
- selftests: watchdog: Fix error message.
- selftests: kvm: Fix -Wformat warnings
- selftests: fix warning: “\_GNU\_SOURCE” redefined
- net: ethernet: cadence: fix socket buffer corruption problem
- bpf: devmap: fix wrong interface selection in notifier\_call
- bpf, btf: fix a missing check bug in btf\_parse
- [sparc64] Rework xchg() definition to avoid warnings.
- [arm64] lib: use C string functions with KASAN enabled
- fs/ocfs2/dlm/dlmdebug.c: fix a sleep-in-atomic-context bug in dlm\_print\_one\_mle()
- mm/page-writeback.c: fix range\_cyclic writeback vs writepages deadlock
- tools/testing/selftests/vm/gup\_benchmark.c: fix ‘write’ flag usage
- mm: thp: fix MADV\_DONTNEED vs migrate\_misplaced\_transhuge\_page race condition
- macsec: update operstate when lower device changes
- macsec: let the administrator set UP state even if lowerdev is down
- block: fix the DISCARD request merge
- i2c: uniphier-f: make driver robust against concurrency
- i2c: uniphier-f: fix occasional timeout error
- i2c: uniphier-f: fix race condition when IRQ is cleared
- um: Make line/tty semantics use true write IRQ
- vfs: avoid problematic remapping requests into partial EOF block
- ipv4/igmp: fix v1/v2 switchback timeout based on rfc3376, 8.12
- [ppc64\*,powerpc] xmon: Relax frame size for clang
- [ppc64\*,powerpc] selftests/ptrace: Fix out-of-tree build
- [ppc64\*,powerpc] selftests/signal: Fix out-of-tree build
- [ppc64\*,powerpc] selftests/switch\_endian: Fix out-of-tree build
- [ppc64\*,powerpc] selftests/cache\_shape: Fix out-of-tree build
- block: call rq\_qos\_exit() after queue is frozen
- mm/gup\_benchmark.c: prevent integer overflow in ioctl
- linux/bitmap.h: handle constant zero-size bitmaps correctly
- linux/bitmap.h: fix type of nbits in bitmap\_shift\_right()
- lib/bitmap.c: fix remaining space computation in bitmap\_print\_to\_pagebuf

- hfsplus: fix BUG on bnode parent update
- hfs: fix BUG on bnode parent update
- hfsplus: prevent btree data loss on ENOSPC
- hfs: prevent btree data loss on ENOSPC
- hfsplus: fix return value of hfsplus\_get\_block()
- hfs: fix return value of hfs\_get\_block()
- hfsplus: update timestamps on truncate()
- hfs: update timestamp on truncate()
- fs/hfs/extent.c: fix array out of bounds read of array extent
- kernel/panic.c: do not append newline to the stack protector panic string
- mm/memory\_hotplug: make add\_memory() take the device\_hotplug\_lock
- mm/memory\_hotplug: fix online/offline\_pages called w.o. mem\_hotplug\_lock
- [ppc64\*,powerpc] powerpc/powernv: hold device\_hotplug\_lock when calling device\_online()
- igb: shorten maximum PHC timecounter update interval
- fm10k: ensure completer aborts are marked as non-fatal after a resume
- [arm64] net: hns3: bugfix for buffer not free problem during resetting
- [arm64] net: hns3: bugfix for reporting unknown vector0 interrupt repeatedly problem
- [arm64] net: hns3: bugfix for is\_valid\_csq\_clean\_head()
- [arm64] net: hns3: bugfix for hclge\_mdio\_write and hclge\_mdio\_read
- ntb\_netdev: fix sleep time mismatch
- [x86] ntb: intel: fix return value for ndev\_vec\_mask()
- irq/matrix: Fix memory overallocation
- nvme-pci: fix conflicting p2p resource adds
- [arm64] makefile fix build of .i file in external module case
- [x86] tools/power/turbosat: fix AMD APIC-id output
- mm: handle no memcg case in memcg\_kmem\_charge() properly
- ocfs2: without quota support, avoid calling quota recovery
- ocfs2: don't use iocb when EIOCBQUEUED returns
- ocfs2: don't put and assigning null to bh allocated outside
- ocfs2: fix clusters leak in ocfs2\_defrag\_extent()
- net: do not abort bulk send on BQL status
- sched/topology: Fix off by one bug
- sched/fair: Don't increase sd->balance\_interval on newidle balance
- openvswitch: fix linking without CONFIG\_NF\_CONNTRACK\_LABELS
- [armhf] dts: imx6sx-sdb: Fix enet phy regulator
- [arm64] sunxi-ng: enable so-said LDOs for A64 SoC's pll-mipi clock

- soc: bcm: brcmstb: Fix re-entry point with a THUMB2\_KERNEL
- audit: print empty EXECVE args
- sock\_diag: fix autoloading of the raw\_diag module
- net: bpfILTER: fix iptables failure if bpfILTER\_umh is disabled
- nds32: Fix bug in bitfield.h
- media: ov13858: Check for possible null pointer
- btrfs: avoid link error with CONFIG\_NO\_AUTO\_INLINE
- wil6210: fix debugfs memory access alignment
- wil6210: fix L2 RX status handling
- wil6210: fix RGF\_CAF\_ICR address for Talyn-MB
- wil6210: fix locking in wmi\_call
- ath10k: snoc: fix unbalanced clock error handling
- wlcore: Fix the return value in case of error in 'wlcore\_vendor\_cmd\_smart\_config\_start()'
- rtl8xxxu: Fix missing break in switch
- brcmsmac: never log "tid x is not agg'able" by default
- wireless: airo: potential buffer overflow in sprintf()
- rtlwifi: rtl8192de: Fix misleading REG\_MCUFWDL information
- net: dsa: bcm\_sf2: Turn on PHY to allow successful registration
- scsi: mpt3sas: Fix Sync cache command failure during driver unload
- scsi: mpt3sas: Don't modify EEDPtagMode field setting on SAS3.5 HBA devices
- scsi: mpt3sas: Fix driver modifying persistent data in Manufacturing page11
- scsi: megaraid\_sas: Fix msleep granularity
- scsi: megaraid\_sas: Fix goto labels in error handling
- scsi: lpfc: fcoe: Fix link down issue after 1000+ link bounces
- scsi: lpfc: Fix odd recovery in duplicate FLOGIs in point-to-point
- scsi: lpfc: Correct loss of fc4 type on remote port address change
- usb: typec: tcpm: charge current handling for sink during hard reset
- dlm: fix invalid free
- dlm: don't leak kernel pointer to userspace
- vrf: mark skb for multicast or link-local as enslaved to VRF
- clk: tegra20: Turn EMC clock gate into divider
- ACPIA: Use %d for signed int print formatting instead of %u
- net: bcmgenet: return correct value 'ret' from bcmgenet\_power\_down
- of: unittest: allow base devicetree to have symbol metadata
- of: unittest: initialize args before calling of\_\*parse\_\*
- tools: bpftool: pass an argument to silence open\_obj\_pinned()

- cfg80211: Prevent regulatory restore during STA disconnect in concurrent interfaces
- pinctrl: qcom: spmi-gpio: fix gpio-hog related boot issues
- pinctrl: bcm2835: Use define directive for BCM2835\_PINCONF\_PARAM\_PULL
- pinctrl: lpc18xx: Use define directive for PIN\_CONFIG\_GPIO\_PIN\_INT
- pinctrl: zynq: Use define directive for PIN\_CONFIG\_IO\_STANDARD
- PCI: keystone: Use quirk to limit MRRS for K2G
- nvme-pci: fix surprise removal
- spi: omap2-mcspi: Fix DMA and FIFO event trigger size mismatch
- i2c: uniphier-f: fix timeout error after reading 8 bytes
- mm/memory\_hotplug: Do not unlock when fails to take the device\_hotplug\_lock
- ipv6: Fix handling of LLA with VRF and sockets bound to VRF
- cfg80211: call disconnect\_wk when AP stops
- mm/page\_io.c: do not free shared swap slots
- Bluetooth: Fix invalid-free in bcbp\_close()
- KVM: MMU: Do not treat ZONE\_DEVICE pages as being reserved
- ath10k: Fix a NULL-ptr-deref bug in ath10k\_usb\_alloc\_urb\_from\_pipe
- ath9k\_hw: fix uninitialized variable data
- md/raid10: prevent access of uninitialized resync\_pages offset
- mm/memory\_hotplug: don't access uninitialized memmaps in shrink\_zone\_span()
- net: phy: dp83867: fix speed 10 in sgmi mode
- net: phy: dp83867: increase SGMII autoneg timer duration
- ocfs2: remove ocfs2\_is\_o2cb\_active()
- [arm\*] 8904/1: skip nomap memblocks while finding the lowmem/highmem boundary
- ARC: perf: Accommodate big-endian CPU
- [x86] insn: Fix awk regex warnings
- [x86] speculation: Fix incorrect MDS/TAA mitigation status
- [x86] speculation: Fix redundant MDS mitigation message
- nbd: prevent memory leak
- y2038: futex: Move compat implementation into futex.c
- futex: Prevent robust futex exit race
- ALSA: usb-audio: Fix NULL dereference at parsing BADD
- nfc: port100: handle command failure cleanly
- media: vivid: Set vid\_cap\_streaming and vid\_out\_streaming to true
- media: vivid: Fix wrong locking that causes race conditions on streaming stop (CVE-2019-18683)
- media: usbvision: Fix races among open, close, and disconnect
- cpufreq: Add NULL checks to show() and store() methods of cpufreq



- media: uvcvideo: Fix error path in control parsing failure
- media: b2c2-flexcop-usb: add sanity checking
- media: cxusb: detect cxusb\_ctrl\_msg error in query
- media: imon: invalid dereference in imon\_touch\_event
- virtio\_ring: fix return code on DMA mapping fails
- USBIP: add config dependency for SGL\_ALLOC
- usbip: tools: fix fd leakage in the function of read\_attr\_usbip\_status
- usbip: Fix uninitialized symbol 'nents' in stub\_recv\_cmd\_submit()
- usb-serial: cp201x: support Mark-10 digital force gauge
- USB: chaoskey: fix error case of a timeout
- appledisplay: fix error handling in the scheduled work
- USB: serial: mos7840: add USB ID to support Moxa UPort 2210
- USB: serial: mos7720: fix remote wakeup
- USB: serial: mos7840: fix remote wakeup
- USB: serial: option: add support for DW5821e with eSIM support
- USB: serial: option: add support for Foxconn T77W968 LTE modules
- staging: comedi: usbduxfast: usbduxfast\_ai\_cmdtest rounding error
- [ppc64\*] support nospectre\_v2 cmdline option
- [ppc64\*] book3s: Fix link stack flush on context switch (CVE-2019-18660)
- [ppc64\*, powerpc] PPC: Book3S HV: Flush link stack on guest exit to host kernel
- PM / devfreq: Fix kernel oops on governor module load

#### Romain Perier

- [armel/rpi] Enable CONFIG\_BRCMFMAC\_SDIO (Closes: #940530)
- [armhf, arm64] Backport devicetree for enabling support for the Raspberry PI 3 A+

#### Salvatore Bonaccorso

- ixgbe: Fix secpath usage for IPsec TX offload (Closes: #930443)
- ipv4: Return -ENETUNREACH if we can't create route but saddr is valid (Closes: #945023)
- [x86] KVM: x86: introduce is\_pae\_paging (Regression in 4.19.77)
- [rt] Refresh 0011-sched-fair-Robustify-CFS-bandwidth-timer-locking.patch (context changes in 4.19.84)

#### Bastian Blank

- [amd64/cloud-amd64] Re-enable RTC drivers. (closes: #931341)

#### Noah Meyerhans

- drivers/net/ethernet/amazon: Backport driver fixes from Linux 5.4 (Closes: #941291)
- Bump ABI to 7

#### Ben Hutchings

- debian/bin/genpatch-rt: Fix series generation from git

- [rt] Update to 4.19.82-rt30:
  - Drop changes in “fs/dcache: disable preemption on i\_dir\_seq’s write side” that conflict with “Fix the locking in dcache\_readdir() and friends”
  - Rewrite “fs/aio: simple simple work” using kthread\_work
  - Rewrite “thermal: Defer thermal wakups to threads” using kthread\_work
  - Rewrite “block: blk-mq: move blk\_queue\_usage\_counter\_release() into process context” using kthread\_work
  - workqueue: rework

Benjamin Poirier

- tools/perf: Add python3 support to scripts (Closes: #944641)

Aurelien Jarno

- [rt] Refresh 0025-NFSv4-replace-seqcount\_t-with-a-seqlock\_t.patch (context changes in 4.19.86)
- [rt] Refresh 0202-net-Qdisc-use-a-seqlock-instead-seqcount.patch (context changes in 4.19.86)
- [rt] Refresh 0057-printk-Add-a-printk-kill-switch.patch (context changes in 4.19.87)
- [rt] Refresh 0207-printk-Make-rt-aware.patch (context changes in 4.19.87)

## 3.15 linux-image-armmp-lpae

### 3.15.1 105+deb10u3 - 31. January 2020

- Update to 4.19.0-8

### 3.15.2 105+deb10u2 - 29. December 2019

- Update to 4.19.0-7

## 3.16 openssh-client

### 3.16.1 1:7.9p1-10+deb10u2 - 31. January 2020

- Apply upstream patch to deny (non-fatally) ipc in the seccomp sandbox, fixing failures with OpenSSL 1.1.1d and Linux < 3.19 on some architectures (closes: #946242). Note that this also drops the previous change to allow ipc on s390, since upstream has security concerns with that and it doesn’t currently seem to be needed.

## 3.17 openssh-server

### 3.17.1 1:7.9p1-10+deb10u2 - 31. January 2020

- Apply upstream patch to deny (non-fatally) ipc in the seccomp sandbox, fixing failures with OpenSSL 1.1.1d and Linux < 3.19 on some architectures (closes: #946242). Note that this also drops the previous change to allow ipc on s390, since upstream has security concerns with that and it doesn’t currently seem to be needed.

## 3.18 openssh-sftp-server

### 3.18.1 1:7.9p1-10+deb10u2 - 31. January 2020

- Apply upstream patch to deny (non-fatally) ipc in the seccomp sandbox, fixing failures with OpenSSL 1.1.1d and Linux < 3.19 on some architectures (closes: #946242). Note that this also drops the previous change to allow ipc on s390, since upstream has security concerns with that and it doesn't currently seem to be needed.

## 3.19 python-apt-common

### 3.19.1 1.8.4.1 - 23. January 2020

- SECURITY UPDATE: Check that repository is trusted before downloading files from it (LP: #1858973)
  - apt/cache.py: Add checks to fetch\_archives() and commit()
  - apt/package.py: Add checks to fetch\_binary() and fetch\_source()
  - CVE-2019-15796
- SECURITY UPDATE: Do not use MD5 for verifying downloadeds (Closes: #944696) (LP: #1858972)
  - apt/package.py: Use all hashes when fetching packages, and check that we have trusted hashes when downloading
  - CVE-2019-15795
- To work around the new checks, the parameter allow\_unauthenticated=True can be passed to the functions. It defaults to the value of the APT::Get::AllowUnauthenticated option.
- Automatic changes and fixes for external regressions:
  - Adjustments to test suite and CI to fix CI regressions
  - testcommon: Avoid reading host apt.conf files
  - Automatic mirror list update

## 3.20 python3-apt

### 3.20.1 1.8.4.1 - 23. January 2020

- SECURITY UPDATE: Check that repository is trusted before downloading files from it (LP: #1858973)
  - apt/cache.py: Add checks to fetch\_archives() and commit()
  - apt/package.py: Add checks to fetch\_binary() and fetch\_source()
  - CVE-2019-15796
- SECURITY UPDATE: Do not use MD5 for verifying downloadeds (Closes: #944696) (LP: #1858972)
  - apt/package.py: Use all hashes when fetching packages, and check that we have trusted hashes when downloading
  - CVE-2019-15795

- To work around the new checks, the parameter `allow_unauthenticated=True` can be passed to the functions. It defaults to the value of the `APT::Get::AllowUnauthenticated` option.
- Automatic changes and fixes for external regressions:
  - Adjustments to test suite and CI to fix CI regressions
  - testcommon: Avoid reading host apt.conf files
  - Automatic mirror list update

## 3.21 python3.7

### 3.21.1 3.7.3-2+deb10u1 - 20. December 2019

- CVE-2019-9740
- CVE-2019-9947
- CVE-2019-9948
- CVE-2019-10160
- CVE-2019-16056
- CVE-2019-16935

## 3.22 python3.7-minimal

### 3.22.1 3.7.3-2+deb10u1 - 20. December 2019

- CVE-2019-9740
- CVE-2019-9947
- CVE-2019-9948
- CVE-2019-10160
- CVE-2019-16056
- CVE-2019-16935

## 3.23 sudo

### 3.23.1 1.8.27-1+deb10u2 - 02. February 2020

- Non-maintainer upload.
- Fix a buffer overflow when pwfeedback is enabled and input is a not a tty (CVE-2019-18634) (Closes: #950371)

## 3.24 systemd

### 3.24.1 241-7~deb10u3 - 29. January 2020

- core: set fs.file-max sysctl to LONG\_MAX rather than ULONG\_MAX. Since kernel 5.2 (but also stable kernels like 4.19.53) the kernel thankfully returns proper errors when we write a value out of range to the sysctl. Which however breaks writing ULONG\_MAX to request the maximum value. Hence let's write the new maximum value instead, LONG\_MAX. (Closes: #945018)
- core: change ownership/mode of the execution directories also for static users. This ensures that execution directories like CacheDirectory and StateDirectory are properly chowned to the user specified in User= before launching the service. (Closes: #919231)

## 3.25 systemd-sysv

### 3.25.1 241-7~deb10u3 - 29. January 2020

- core: set fs.file-max sysctl to LONG\_MAX rather than ULONG\_MAX. Since kernel 5.2 (but also stable kernels like 4.19.53) the kernel thankfully returns proper errors when we write a value out of range to the sysctl. Which however breaks writing ULONG\_MAX to request the maximum value. Hence let's write the new maximum value instead, LONG\_MAX. (Closes: #945018)
- core: change ownership/mode of the execution directories also for static users. This ensures that execution directories like CacheDirectory and StateDirectory are properly chowned to the user specified in User= before launching the service. (Closes: #919231)

## 3.26 udev

### 3.26.1 241-7~deb10u3 - 29. January 2020

- core: set fs.file-max sysctl to LONG\_MAX rather than ULONG\_MAX. Since kernel 5.2 (but also stable kernels like 4.19.53) the kernel thankfully returns proper errors when we write a value out of range to the sysctl. Which however breaks writing ULONG\_MAX to request the maximum value. Hence let's write the new maximum value instead, LONG\_MAX. (Closes: #945018)
- core: change ownership/mode of the execution directories also for static users. This ensures that execution directories like CacheDirectory and StateDirectory are properly chowned to the user specified in User= before launching the service. (Closes: #919231)