JSA103137 Session Smart Router: Multiple vulnerabilities resolved in Session Smart Router 6.2.10-lts, 6.3.6-STS

Multiple vulnerabilities have been resolved in Juniper Networks Session Smart Router 6.2.10-lts, 6.3.6-sts by updating third-party software included with Session Smart Router.

These issues affect all versions of Session Smart Router before 6.2.10-lts, 6.3.6-sts.

PRODUCT AFFECTED:

This issue affects Session Smart Router 0, 6.3.0. Affected platforms: .

Problem:

Important security issues resolved include:

CVE	CVSS	Summary
CVE-2016-9840	8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.
CVE-2020-12321	8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	Improper buffer restriction in some Intel(R) Wireless Bluetooth(R) products before version 21.110 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.
CVE-2020-22218	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	An issue was discovered in function _libssh2_packet_add in libssh2 1.10.0 allows attackers to access out of bounds memory.

CVE-2021-26341	6.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)	Some AMD CPUs may transiently execute beyond unconditional direct branches, which may potentially result in data leakage.
CVE-2021-33655	6.7 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	When sending malicous data to kernel by ioctl cmd FBIOPUT_VSCREENINFO,kernel will write memory out of bounds.
CVE-2021-33656	6.8 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	When setting font with malicous data by ioctl cmd PIO_FONT,kernel will write memory out of bounds.
CVE-2021-43975	6.7 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel through 5.15.2, hw_atl_utils_fw_rpc_wait in drivers/net/ethernet/aquantia/atlantic/hw_atl/hw_atl_utils.c allows an attacker (who can introduce a crafted device) to trigger an out-of-bounds write via a crafted length value.
CVE-2021-46	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: tracing: Restructure trace_clock_global() to never block It was reported that a fix to the ring buffer recursion detection would cause a hung machine when performing suspend / resume testing. The following

939		backtrace was extracted from debugging that case: Call Trace: trace_clock_global+0x91/0xa0 __rb_reserve_next+0x237/0x460 ring_buffer_lock_reserve+0x12a/0x3f0 trace_buffer_lock_reserve+0x10/0x50 __trace_graph_return+0x1f/0x80 trace_graph_return+0xb7/0xf0 ? trace_clock_global+0x91/0xa0 ftrace_return_to_handler+0x8b/0xf0 ? pv_hash+0xa0/0xa0 return_to_handler+0x15/0x30 ? ftrace_graph_caller+0xa0/0xa0 ? trace_clock_global+0x91/0xa0 ? __rb_reserve_next+0x237/0x460 ? ring_buffer_lock_reserve+0x12a/0x3f0 ? trace_event_buffer_lock_reserve+0x3c/0x120 ? trace_event_buffer_reserve+0x6b/0xc0 ? trace_event_raw_event_device_pm_callback_start+0x125 /0x2d0 ? dpm_run_callback+0x3b/0xc0 ? pm_ops_is_empty+0x50/0x50 ? platform_get_irq_byname_optional+0x90/0x90 ? trace_device_pm_callback_start+0x82/0xd0 ? dpm_run_callback+0x49/0xc0 With the following RIP: RIP: 0010:native_queued_spin_lock_slowpath+0x69/0x200 Since the fix to the recursion detection would allow a single recursion to happen while tracing, this lead to the trace_clock_global() taking a spin lock and then trying to take it again: ring_buffer_lock_reserve() { trace_clock_global() { arch_spin_lock() { queued_spin_lock_slowpath() { /* lock taken */ (something else gets traced by function graph tracer) ring_buffer_lock_reserve() { trace_clock_global() { arch_spin_lock() { queued_spin_lock_slowpath() { /* DEAD LOCK! */ Tracing should *never* block, as it can lead to strange lockups like the above. Restructure the trace_clock_global() code to instead of simply taking a lock to update the recorded "prev_time" simply use it, as two events happening on two different CPUs that calls this

		at the same time, really doesn't matter which one goes first. Use a trylock to grab the lock for updating the prev_time, and if it fails, simply try again the next time. If it failed to be taken, that means something else is already updating it. Bugzilla: https://bugzilla.kernel.org/show_bug.cgi?id=212761
CVE-2021-47018	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: powerpc/64: Fix the definition of the fixmap area At the time being, the fixmap area is defined at the top of the address space or just below KASAN. This definition is not valid for PPC64. For PPC64, use the top of the I/O space. Because of circular dependencies, it is not possible to include asm/fixmap.h in asm/book3s/64/pgtable.h , so define a fixed size AREA at the top of the I/O space for fixmap and ensure during build that the size is big enough.
CVE-2021-47257	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: net: ieee802154: fix null deref in parse dev addr Fix a logic error that could result in a null deref if the user sets the mode incorrectly for the given addr type.
CVE-2021-47284	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: isdn: mISDN: netjet: Fix crash in nj_probe: 'nj_setup' in netjet.c might fail with -EIO and in this case 'card->irq' is initialized and is bigger than zero. A subsequent call to 'nj_release' will free the irq that has not been requested. Fix this bug by deleting the previous assignment to 'card->irq' and just keep the assignment before 'request_irq'. The KASAN's log reveals it: [3.354615] WARNING: CPU: 0 PID: 1 at kernel/irq/manage.c:1826 free_irq+0x100/0x480 [3.355112] Modules linked in: [3.355310] CPU: 0 PID: 1

		Comm: swapper/0 Not tainted 5.13.0-rc1-00144-g25a1298726e #13 [3.355816] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.12.0-59-gc9ba5276e321-prebuilt.qemu.org 04/01/2014 [3.356552] RIP: 0010:free_irq+0x100/0x480 [3.356820] Code: 6e 08 74 6f 4d 89 f4 e8 5e ac 09 00 4d 8b 74 24 18 4d 85 f6 75 e3 e8 4f ac 09 00 8b 75 c8 48 c7 c7 78 c1 2e 85 e8 e0 cf f5 ff <0f> 0b 48 8b 75 c0 4c 89 ff e8 72 33 0b 03 48 8b 43 40 4c 8b a0 80 [3.358012] RSP: 0000:ffffc90000017b48 EFLAGS: 00010082 [3.358357] RAX: 0000000000000000 RBX: ffff888104dc8000 RCX: 0000000000000000 [3.358814] RDX: ffff8881003c8000 RSI: ffffffff8124a9e6 RDI: 00000000ffffffff [3.359272] RBP: ffffc90000017b88 R08: 0000000000000000 R09: 0000000000000000 [3.359732] R10: ffffc900000179f0 R11: 0000000000001d04 R12: 0000000000000000 [3.360195] R13: ffff888107dc6000 R14: ffff888107dc6928 R15: ffff888104dc80a8 [3.360652] FS: 0000000000000000(0000) GS:ffff88817bc00000(0000) knlGS:0000000000000000 [3.361170] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [3.361538] CR2: 0000000000000000 CR3: 000000000582e000 CR4: 00000000000006f0 [3.362003] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [3.362175] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [3.362175] Call Trace: [3.362175] nj_release+0x51/0x1e0 [3.362175] nj_probe+0x450/0x950 [3.362175] ? pci_device_remove+0x110/0x110 [3.362175] local_pci_probe+0x45/0xa0 [3.362175] pci_device_probe+0x12b/0x1d0 [3.362175] really_probe+0x2a9/0x610 [3.362175] driver_probe_device+0x90/0x1d0 [3.362175] ? mutex_lock_nested+0x1b/0x20 [3.362175] device_driver_attach+0x68/0x70 [3.362175] __driver_attach+0x124/0x1b0 [3.362175] ? device_driver_attach+0x70/0x70 [3.362175]

		bus_for_each_dev+0xbb/0x110 [3.362175] ? rdinit_setup+0x45/0x45 [3.362175] driver_attach+0x27/0x30 [3.362175] bus_add_driver+0x1eb/0x2a0 [3.362175] driver_register+0xa9/0x180 [3.362175] __pci_register_driver+0x82/0x90 [3.362175] ? w6692_init+0x38/0x38 [3.362175] nj_init+0x36/0x38 [3.362175] do_one_initcall+0x7f/0x3d0 [3.362175] ? rdinit_setup+0x45/0x45 [3.362175] ? rcu_read_lock_sched_held+0x4f/0x80 [3.362175] kernel_init_freeable+0x2aa/0x301 [3.362175] ? rest_init+0x2c0/0x2c0 [3.362175] kernel_init+0x18/0x190 [3.362175] ? rest_init+0x2c0/0x2c0 [3.362175] ? rest_init+0x2c0/0x2c0 [3.362175] ret_from_fork+0x1f/0x30 [3.362175] Kernel panic - not syncing: panic_on_warn set ... [3.362175] CPU: 0 PID: 1 Comm: swapper/0 Not tainted 5.13.0-rc1-00144-g25a1298726e #13 [3.362175] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.12.0-59-gc9ba5276e321-prebuilt.qemu.org 04/01/2014 [3.362175] Call Trace: [3.362175] dump_stack+0xba/0xf5 [3.362175] ? free_irq+0x100/0x480 [3.362175] panic+0x15a/0x3f2 [3.362175] ? __warn+0xf2/0x150 [3.362175] ? free_irq+0x100/0x480 [3.362175] __warn+0x108/0x150 [3.362175] ? free_irq+0x100/0x480 [3.362175] report_bug+0x119/0x1c0 [3.362175] handle_bug+0x3b/0x80 [3.362175] exc_invalid_op+0x18/0x70 [3.362175] asm_exc_invalid_op+0x12/0x20 [3.362175] RIP: 0010:free_irq+0x100 ---truncated---
CVE-2021-	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: tcp: fix tcp_init_transfer() to not reset icsk_ca_initialized This commit fixes a bug (found by syzkaller) that could cause spurious double-initializations

4730 4		for congestion control modules, which could cause memory leaks or other problems for congestion control modules (like CDG) that allocate memory in their init functions. The buggy scenario constructed by syzkaller was something like: (1) create a TCP socket (2) initiate a TFO connect via sendto() (3) while socket is in TCP_SYN_SENT, call setsockopt(TCP_CONGESTION), which calls: tcp_set_congestion_control() -> tcp_reinit_congestion_control() -> tcp_init_congestion_control() (4) receive ACK, connection is established, call tcp_init_transfer(), set icsk_ca_initialized=0 (without first calling cc->release()), call tcp_init_congestion_control() again. Note that in this sequence tcp_init_congestion_control() is called twice without a cc->release() call in between. Thus, for CC modules that allocate memory in their init() function, e.g, CDG, a memory leak may occur. The syzkaller tool managed to find a reproducer that triggered such a leak in CDG. The bug was introduced when that commit 8919a9b31eb4 ("tcp: Only init congestion control if not initialized already") introduced icsk_ca_initialized and set icsk_ca_initialized to 0 in tcp_init_transfer(), missing the possibility for a sequence like the one above, where a process could call setsockopt(TCP_CONGESTION) in state TCP_SYN_SENT (i.e. after the connect() or TFO open sendmsg()), which would call tcp_init_congestion_control(). It did not intend to reset any initialization that the user had already explicitly made; it just missed the possibility of that particular sequence (which syzkaller managed to find).
CVE-2021-47	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: irqchip/gic-v3-its: Fix potential VPE leak on error In its_vpe_irq_domain_alloc, when its_vpe_init() returns an error, there is an off-by-one in the number of VPEs to be freed. Fix it by simply passing the number of VPEs

373		allocated, which is the index of the loop iterating over the VPEs. [maz: fixed commit message]
CVE-2021-47408	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: netfilter: conntrack: serialize hash resizes and cleanups Syzbot was able to trigger the following warning [1] No repro found by syzbot yet but I was able to trigger similar issue by having 2 scripts running in parallel, changing conntrack hash sizes, and: for j in `seq 1 1000` ; do unshare -n /bin/true >/dev/null ; done It would take more than 5 minutes for net_namespace structures to be cleaned up. This is because nf_ct_iterate_cleanup() has to restart everytime a resize happened. By adding a mutex, we can serialize hash resizes and cleanups and also make get_next_corpse() faster by skipping over empty buckets. Even without resizes in the picture, this patch considerably speeds up network namespace dismantles. [1] INFO: task syz-executor.0:8312 can't die for more than 144 seconds. task:syz-executor.0 state:R running task stack:25672 pid: 8312 ppid: 6573 flags:0x00004006 Call Trace: context_switch kernel/sched/core.c:4955 [inline] __schedule+0x940/0x26f0 kernel/sched/core.c:6236 preempt_schedule_common+0x45/0xc0 kernel/sched/core.c:6408 preempt_schedule_thunk+0x16/0x18 arch/x86/entry/thunk_64.S:35 __local_bh_enable_ip+0x109/0x120 kernel/softirq.c:390 local_bh_enable include/linux/bottom_half.h:32 [inline] get_next_corpse net/netfilter/nf_conntrack_core.c:2252 [inline] nf_ct_iterate_cleanup+0x15a/0x450 net/netfilter/nf_conntrack_core.c:2275 nf_conntrack_cleanup_net_list+0x14c/0x4f0 net/netfilter/nf_conntrack_core.c:2469 ops_exit_list+0x10d/0x160 net/core/net_namespace.c:171 setup_net+0x639/0xa30 net/core/net_namespace.c:349 copy_net_ns+0x319/0x760

		net/core/net_namespace.c:470 create_new_namespaces+0x3f6/0xb20 kernel/nsproxy.c:110 unshare_nsproxy_namespaces+0xc1/0x1f0 kernel/nsproxy.c:226 ksys_unshare+0x445/0x920 kernel/fork.c:3128 __do_sys_unshare kernel/fork.c:3202 [inline] __se_sys_unshare kernel/fork.c:3200 [inline] __x64_sys_unshare+0x2d/0x40 kernel/fork.c:3200 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f63da68e739 RSP: 002b:00007f63d7c05188 EFLAGS: 00000246 ORIG_RAX: 0000000000000110 RAX: ffffffffffffffda RBX: 00007f63da792f80 RCX: 00007f63da68e739 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000040000000 RBP: 00007f63da6e8cc4 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 00007f63da792f80 R13: 00007fff50b75d3f R14: 00007f63d7c05300 R15: 0000000000022000 Showing all locks held in the system: 1 lock held by khungtaskd/27: #0: ffffffff8b980020 (rcu_read_lock){....}-{1:2}, at: debug_show_all_locks+0x53/0x260 kernel/locking/lockdep.c:6446 2 locks held by kworker/u4:2/153: #0: ffff888010c69138 ((wq_completion)events_unbound){+.+.}-{0:0}, at: arch_atomic64_set arch/x86/include/asm/atomic64_64.h:34 [inline] #0: ffff888010c69138 ((wq_completion)events_unbound){+.+.}-{0:0}, at: arch_atomic_long_set include/linux/atomic/atomic-long.h:41 [inline] #0: ffff888010c69138 ((wq_completion)events_unbound){+.+.}-{0:0}, at: atomic_long_set include/linux/atomic/atomic-instrumented.h:1198 [inline] #0: ffff888010c69138 ((wq_completion)events_unbound){+.+.}-{0:0}, at:

		set_work_data kernel/workqueue.c:634 [inline] #0: ffff888010c69138 ((wq_completion)events_unbound){+.+.}-{0:0}, at: set_work_pool_and_clear_pending kernel/workqueue.c:661 [inline] #0: ffff888010c69138 ((wq_completion)events_unbound){+.+.}-{0:0}, at: process_one_work+0x896/0x1690 kernel/workqueue.c:2268 #1: ffffc9000140fdb0 ((kfence_timer).work){+.+.}-{0:0}, at: process_one_work+0x8ca/0x1690 kernel/workqueue.c:2272 1 lock held by systemd-udevd/2970: 1 lock held by in:imklog/6258: #0: ffff88807f970ff0 (&f->f_pos_lock){+.+.}-{3:3}, at: __fdget_pos+0xe9/0x100 fs/file.c:990 3 locks held by kworker/1:6/8158: 1 lock held by syz-executor.0/8312: 2 locks held by kworker/u4:13/9320: 1 lock held by ---truncated---
CVE-2021-47461	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: userfaultfd: fix a race between writeprotect and exit_mmap() A race is possible when a process exits, its VMAs are removed by exit_mmap() and at the same time userfaultfd_writeprotect() is called. The race was detected by KASAN on a development kernel, but it appears to be possible on vanilla kernels as well. Use mmget_not_zero() to prevent the race as done in other userfaultfd operations.
CVE-2021-47468	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: isdn: mISDN: Fix sleeping function called from invalid context The driver can call card->isac.release() function from an atomic context. Fix this by calling this function after releasing the lock. The following log reveals it: [44.168226] BUG: sleeping function called from invalid context at kernel/workqueue.c:3018 [44.168941] in_atomic(): 1, irqs_disabled(): 1, non_block: 0, pid: 5475, name: modprobe [44.169574] INFO: lockdep is turned

		off. [44.169899] irq event stamp: 0 [44.170160] hardirqs last enabled at (0): [<0000000000000000>] 0x0 [44.170627] hardirqs last disabled at (0): [<ffffffff814209ed>] copy_process+0x132d/0x3e00 [44.171240] softirqs last enabled at (0): [<ffffffff81420a1a>] copy_process+0x135a/0x3e00 [44.171852] softirqs last disabled at (0): [<0000000000000000>] 0x0 [44.172318] Preemption disabled at: [44.172320] [<ffffffffa009b0a9>] nj_release+0x69/0x500 [netjet] [44.174441] Call Trace: [44.174630] dump_stack_lvl+0xa8/0xd1 [44.174912] dump_stack+0x15/0x17 [44.175166] ___might_sleep+0x3a2/0x510 [44.175459] ? nj_release+0x69/0x500 [netjet] [44.175791] __might_sleep+0x82/0xe0 [44.176063] ? start_flush_work+0x20/0x7b0 [44.176375] start_flush_work+0x33/0x7b0 [44.176672] ? trace_irq_enable_rcuidle+0x85/0x170 [44.177034] ? kasan_quarantine_put+0xaa/0x1f0 [44.177372] ? kasan_quarantine_put+0xaa/0x1f0 [44.177711] __flush_work+0x11a/0x1a0 [44.177991] ? flush_work+0x20/0x20 [44.178257] ? lock_release+0x13c/0x8f0 [44.178550] ? __kasan_check_write+0x14/0x20 [44.178872] ? do_raw_spin_lock+0x148/0x360 [44.179187] ? read_lock_is_recursive+0x20/0x20 [44.179530] ? __kasan_check_read+0x11/0x20 [44.179846] ? do_raw_spin_unlock+0x55/0x900 [44.180168] ? ____kasan_slab_free+0x116/0x140 [44.180505] ? _raw_spin_unlock_irqrestore+0x41/0x60 [44.180878] ? skb_queue_purge+0x1a3/0x1c0 [44.181189] ? kfree+0x13e/0x290 [44.181438] flush_work+0x17/0x20 [44.181695] mISDN_freedchannel+0xe8/0x100 [44.182006] isac_release+0x210/0x260 [mISDNipac] [44.182366] nj_release+0xf6/0x500 [netjet] [44.182685] nj_remove+0x48/0x70 [netjet] [44.182989] pci_device_remove+0xa9/0x250

CVE-2021-47491	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: mm: khugepaged: skip huge page collapse for special files The read-only THP for filesystems will collapse THP for files opened readonly and mapped with VM_EXEC. The intended usecase is to avoid TLB misses for large text segments. But it doesn't restrict the file types so a THP could be collapsed for a non-regular file, for example, block device, if it is opened readonly and mapped with EXEC permission. This may cause bugs, like [1] and [2]. This is definitely not the intended usecase, so just collapse THP for regular files in order to close the attack surface. [shy828301@gmail.com: fix vm_file check [3]]
CVE-2021-47548	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: ethernet: hisilicon: hns: hns_dsaf_misc: fix a possible array overflow in hns_dsaf_ge_srst_by_port() The if statement: if (port >= DSAF_GE_NUM) return; limits the value of port less than DSAF_GE_NUM (i.e., 8). However, if the value of port is 6 or 7, an array overflow could occur: port_rst_off = dsaf_dev->mac_cb[port]->port_rst_off; because the length of dsaf_dev->mac_cb is DSAF_MAX_PORT_NUM (i.e., 6). To fix this possible array overflow, we first check port and if it is greater than or equal to DSAF_MAX_PORT_NUM, the function returns.
CVE-2021-47579	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: ovl: fix warning in ovl_create_real() Syzbot triggered the following warning in ovl_workdir_create() -> ovl_create_real(): if (!err && WARN_ON(!newdentry->d_inode)) { The reason is that the cgroup2 filesystem returns from mkdir without instantiating the new dentry. Weird filesystems such as this will be rejected by overlayfs at a later stage during setup, but to prevent such a warning, call ovl_mkdir_real() directly from ovl_workdir_create() and reject this case early.

CVE-2021-476224	7.1 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: net/sunrpc: fix reference count leaks in rpc_sysfs_xprt_state_change The refcount leak issues take place in an error handling path. When the 3rd argument buf doesn't match with "offline", "online" or "remove", the function simply returns -EINVAL and forgets to decrease the reference count of a rpc_xprt object and a rpc_xprt_switch object increased by rpc_sysfs_xprt_kobj_get_xprt() and rpc_sysfs_xprt_kobj_get_xprt_switch(), causing reference count leaks of both unused objects. Fix this issue by jumping to the error handling path labelled with out_put when buf matches none of "offline", "online" or "remove".
CVE-2022-090934	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	A single-byte, non-arbitrary write/use-after-free flaw was found in dnsmasq. This flaw allows an attacker who sends a crafted packet processed by dnsmasq, potentially causing a denial of service.
CVE-2022-131304	7.8 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	An out-of-bounds read/write vulnerability was found in e2fsprogs 1.46.5. This issue leads to a segmentation fault and possibly arbitrary code execution via a specially crafted filesystem.
CVE-2022-141462	6.3 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H)	An out-of-bounds read flaw was found in the Linux kernel’s TeleTYpe subsystem. The issue occurs in how a user triggers a race condition using ioctls TIOCSPTLCK and TIOCGPTPEER and TIOCSTI and TCXONC with leakage of memory in the flush_to_ldisc function. This flaw allows a local user to crash the system or read unauthorized random data from memory.

CVE-2022-1679	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A use-after-free flaw was found in the Linux kernel's Atheros wireless adapter driver in the way a user forces the ath9k_htc_wait_for_target function to fail with some input messages. This flaw allows a local user to crash or potentially escalate their privileges on the system.
CVE-2022-1789	6.8 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	With shadow paging enabled, the INVPCID instruction results in a call to kvm_mmu_invpcid_gva. If INVPCID is executed with CR0.PG=0, the invlpg callback is not set and the result is a NULL pointer dereference.
CVE-2022-20141	7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	In ip_check_mc_rcu of igmp.c, there is a possible use after free due to improper locking. This could lead to local escalation of privilege when opening and closing inet sockets with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-112551163References: Upstream kernel
CVE-2022-2196	8.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)	A regression exists in the Linux Kernel within KVM: nVMX that allowed for speculative execution attacks. L2 can carry out Spectre v2 attacks on L1 due to L1 thinking it doesn't need retpolines or IBPB after running L2 due to KVM (L0) advertising eIBRS support to L1. An attacker at L2 with code execution can execute code on an indirect branch on the host machine. We recommend upgrading to Kernel 6.2 or past commit 2e7eab81425a
CVE-2022-25	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel through 5.16.10, certain binary files may have the exec-all attribute if they were built in approximately 2003 (e.g., with GCC 3.2.2 and Linux kernel 2.4.20). This can cause execution of bytes located in supposedly non-executable regions of a file.

265		
CVE-2022-2601	8.6 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)	A buffer overflow was found in grub_font_construct_glyph(). A malicious crafted pf2 font can lead to an overflow when calculating the max_glyph_size value, allocating a smaller than needed buffer for the glyph, this further leads to a buffer overflow and a heap based out-of-bounds write. An attacker may use this vulnerability to circumvent the secure boot mechanism.
CVE-2022-2663	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)	An issue was found in the Linux kernel in nf_conntrack_irc where the message handling can be confused and incorrectly matches the message. A firewall may be able to be bypassed when users are using unencrypted IRC with nf_conntrack_irc configured.
CVE-2022-2838	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	usb_8dev_start_xmit in drivers/net/can/usb/usb_8dev.c in the Linux kernel through 5.17.1 has a double free.
CVE-2022-3028	7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	A race condition was found in the Linux kernel's IP framework for transforming packets (XFRM subsystem) when multiple calls to xfrm_probe_algs occurred simultaneously. This flaw could allow a local attacker to potentially trigger an out-of-bounds write or leak kernel heap memory by performing an out-of-bounds read and copying it into a socket.

CVE-2022-3059 4	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	The Linux kernel before 5.17.2 mishandles seccomp permissions. The PTRACE_SEIZE code path allows attackers to bypass intended restrictions on setting the PT_SUSPEND_SECCOMP flag.
CVE-2022-3239	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A flaw use after free in the Linux kernel video4linux driver was found in the way user triggers em28xx_usb_probe() for the Empia 28xx based TV cards. A local user could use this flaw to crash the system or potentially escalate their privileges on the system.
CVE-2022-3522		Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.
CVE-2022-3524	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function ipv6_renew_options of the component IPv6 Handler. The manipulation leads to memory leak. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211021 was assigned to this vulnerability.
CVE-2022-3564	7.1 (CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	A vulnerability classified as critical was found in Linux Kernel. Affected by this vulnerability is the function l2cap_reassemble_sdu of the file net/bluetooth/l2cap_core.c of the component Bluetooth. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211087.

CVE-2022-3566	7.1 (CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	A vulnerability, which was classified as problematic, was found in Linux Kernel. This affects the function tcp_getsockopt/tcp_setsockopt of the component TCP Handler. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. The identifier VDB-211089 was assigned to this vulnerability.
CVE-2022-3567	6.4 (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H)	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function inet6_stream_ops/inet6_dgram_ops of the component IPv6 Handler. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. VDB-211090 is the identifier assigned to this vulnerability.
CVE-2022-3594	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)	A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function intr_callback of the file drivers/net/usb/r8152.c of the component BPF. The manipulation leads to logging of excessive data. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211363.
CVE-2022-3619	4.3 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function l2cap_recv_acldata of the file net/bluetooth/l2cap_core.c of the component Bluetooth. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. VDB-211918 is the identifier assigned to this vulnerability.
CVE-2022-	7.5 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function follow_page_pte of the file mm/gup.c of the component BPF. The manipulation leads to race condition. The attack can be launched remotely. It is recommended

3623		to apply a patch to fix this issue. The identifier VDB-211921 was assigned to this vulnerability.
CVE-2022-3625	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A vulnerability was found in Linux Kernel. It has been classified as critical. This affects the function devlink_param_set/devlink_param_get of the file net/core/devlink.c of the component IPsec. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier VDB-211929 was assigned to this vulnerability.
CVE-2022-3628	6.6 (CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A buffer overflow flaw was found in the Linux kernel Broadcom Full MAC Wi-Fi driver. This issue occurs when a user connects to a malicious USB device. This can allow a local user to crash the system or escalate their privileges.
CVE-2022-3640	8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	A vulnerability, which was classified as critical, was found in Linux Kernel. Affected is the function l2cap_conn_del of the file net/bluetooth/l2cap_core.c of the component Bluetooth. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211944.
CVE-2022-3707	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A double-free memory flaw was found in the Linux kernel. The Intel GVT-g graphics driver triggers VGA card system resource overload, causing a fail in the intel_gvt_dma_map_guest_page function. This issue could allow a local user to crash the system.
CVE-2022-37	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to

434		call inflateGetHeader (e.g., see the nodejs/node reference).
CVE-2022-38023	8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	Netlogon RPC Elevation of Privilege Vulnerability
CVE-2022-38457	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A use-after-free(UAF) vulnerability was found in function 'vmw_cmd_res_check' in drivers/gpu/vmxgfx/vmxgfx_execbuf.c in Linux kernel's vmwgfx driver with device file '/dev/dri/renderD128 (or Dxxx)'. This flaw allows a local attacker with a user account on the system to gain privilege, causing a denial of service(DoS).
CVE-2022-39188	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)	An issue was discovered in include/asm-generic/tlb.h in the Linux kernel before 5.19. Because of a race condition (unmap_mapping_range versus munmap), a device driver can free a page while it still has stale TLB entries. This only occurs in situations with VM_PFNMAP VMAs.
CVE-2022-39189	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	An issue was discovered the x86 KVM subsystem in the Linux kernel before 5.18.17. Unprivileged guest users can compromise the guest kernel because TLB flush operations are mishandled in certain KVM_VCPU_PREEMPTED situations.

CVE-2022-40133	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A use-after-free(UAF) vulnerability was found in function 'vmw_execbuf_tie_context' in drivers/gpu/vmxgfx/vmxgfx_execbuf.c in Linux kernel's vmwgfx driver with device file '/dev/dri/renderD128 (or Dxxx)'. This flaw allows a local attacker with a user account on the system to gain privilege, causing a denial of service(DoS).
CVE-2022-40982	6.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)	Information exposure through microarchitectural state after transient execution in certain vector execution units for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-4121 8	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In drivers/media/dvb-core/dmxdev.c in the Linux kernel through 5.19.10, there is a use-after-free caused by refcount races, affecting dvb_demux_open and dvb_dmxdev_release.
CVE-2022-4129	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A flaw was found in the Linux kernel's Layer 2 Tunneling Protocol (L2TP). A missing lock when clearing sk_user_data can lead to a race condition and NULL pointer dereference. A local user could use this flaw to potentially crash the system causing a denial of service.
CVE-2022-41	8.1 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)	An issue was discovered in the Linux kernel before 5.19.16. Attackers able to inject WLAN frames could cause a buffer overflow in the ieee80211_bss_info_update function in net/mac80211/scan.c.

674		
CVE-2022-41741	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module.
CVE-2022-41742	7.1 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module.
CVE-2022-41	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	multipath-tools 0.7.0 through 0.9.x before 0.9.2 allows local users to obtain root access, as exploited alone or in conjunction with CVE-2022-41973. Local users able to write to UNIX domain sockets can bypass access controls and manipulate the multipath setup. This can lead to local privilege escalation to root. This occurs because an

974		attacker can repeat a keyword, which is mishandled because arithmetic ADD is used instead of bitwise OR.
CVE-2022-42703	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	mm/rmap.c in the Linux kernel before 5.19.7 has a use-after-free related to leaf anon_vma double reuse.
CVE-2022-42720	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	Various refcounting bugs in the multi-BSS handling in the mac80211 stack in the Linux kernel 5.1 through 5.19.x before 5.19.16 could be used by local attackers (able to inject WLAN frames) to trigger use-after-free conditions to potentially execute code.
CVE-2022-42721	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A list management bug in BSS handling in the mac80211 stack in the Linux kernel 5.1 through 5.19.x before 5.19.16 could be used by local attackers (able to inject WLAN frames) to corrupt a linked list and, in turn, potentially execute code.
CVE-2022-42722	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel 5.8 through 5.19.x before 5.19.16, local attackers able to inject WLAN frames into the mac80211 stack could cause a NULL pointer dereference denial-of-service attack against the beacon protection of P2P devices.

CVE-2022-42895	6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	There is an infoleak vulnerability in the Linux kernel's net/bluetooth/l2cap_core.c's l2cap_parse_conf_req function which can be used to leak kernel pointers remotely. We recommend upgrading past commit https://github.com/torvalds/linux/commit/b1a2cd50c0357f243b7435a732b4e62ba3157a2e https://www.google.com/url
CVE-2022-42896	8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	There are use-after-free vulnerabilities in the Linux kernel's net/bluetooth/l2cap_core.c's l2cap_connect and l2cap_le_connect_req functions which may allow code execution and leaking kernel memory (respectively) remotely via Bluetooth. A remote attacker could execute code leaking kernel memory via Bluetooth if within proximity of the victim. We recommend upgrading past commit https://www.google.com/url https://github.com/torvalds/linux/commit/711f8c3fb3db61897080468586b970c87c61d9e4 https://www.google.com/url
CVE-2022-43552	5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)	A use after free vulnerability exists in curl <7.87.0. Curl can be asked to *tunnel* virtually all protocols it supports through an HTTP proxy. HTTP proxies can (and often do) deny such tunnel operations. When getting denied to tunnel the specific protocols SMB or TELNET, curl would use a heap-allocated struct after it had been freed, in its transfer shutdown code path.
CVE-2022-43750	6.7 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	drivers/usb/mon/mon_bin.c in usbmon in the Linux kernel before 5.19.15 and 6.x before 6.0.1 allows a user-space client to corrupt the monitor's internal memory.

CVE-2022-45869	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A race condition in the x86 KVM subsystem in the Linux kernel through 6.1-rc6 allows guest OS users to cause a denial of service (host OS crash or host OS memory corruption) when nested virtualisation and the TDP MMU are enabled.
CVE-2022-45884	7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvbdev.c has a use-after-free, related to dvb_register_device dynamically allocating fops.
CVE-2022-45886	7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_net.c has a .disconnect versus dvb_device_open race condition that leads to a use-after-free.
CVE-2022-45887	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)	An issue was discovered in the Linux kernel through 6.0.9. drivers/media/usb/ttusb-dec/ttusb_dec.c has a memory leak because of the lack of a dvb_frontend_detach call.
CVE-2022-45	7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	An issue was discovered in the Linux kernel through 6.0.10. In drivers/media/dvb-core/dvb_ca_en50221.c, a use-after-free can occur is there is a disconnect after an open, because of the lack of a wait_event.

919		
CVE-2022-4744	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A double-free flaw was found in the Linux kernel's TUN/TAP device driver functionality in how a user registers the device when the register_netdevice function fails (NETDEV_REGISTER notifier). This flaw allows a local user to crash or potentially escalate their privileges on the system.
CVE-2022-47929	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel before 6.1.6, a NULL pointer dereference bug in the traffic control subsystem allows an unprivileged user to trigger a denial of service (system crash) via a crafted traffic control configuration that is set up with "tc qdisc" and "tc class" commands. This affects qdisc_graft in net/sched/sch_api.c.
CVE-2022-48632	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: i2c: mlxbf: prevent stack overflow in mlxbf_i2c_smbus_start_transaction() memcpy() is called in a loop while 'operation->length' upper bound is not checked and 'data_idx' also increments.
CVE-2022-48743	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: net: amd-xgbe: Fix skb data length underflow There will be BUG_ON() triggered in include/linux/skbuff.h leading to intermittent kernel panic, when the skb length underflow is detected. Fix this by dropping the packet if such length underflows are seen because of inconsistencies in the hardware descriptors.
CVE-20	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	In the Linux kernel, the following vulnerability has been resolved: block: Fix wrong offset in bio_truncate() bio_truncate() clears the buffer outside of last block of

22-48747		bdev, however current bio_truncate() is using the wrong offset of page. So it can return the uninitialized data. This happened when both of truncated/corrupted FS and userspace (via bdev) are trying to read the last of bdev.
CVE-2022-48757	7.1 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: net: fix information leakage in /proc/net/ptype In one net namespace, after creating a packet socket without binding it to a device, users in other net namespaces can observe the new `packet_type` added by this packet socket by reading `/proc/net/ptype` file. This is minor information leakage as packet socket is namespace aware. Add a net pointer in `packet_type` to keep the net namespace of of corresponding packet socket. In `ptype_seq_show`, this net pointer must be checked when it is not NULL.
CVE-2022-49011	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: hwmon: (coretemp) fix pci device refcount leak in nv1a_ram_new() As comment of pci_get_domain_bus_and_slot() says, it returns a pci device with refcount increment, when finish using it, the caller must decrement the reference count by calling pci_dev_put(). So call it after using to avoid refcount leak.
CVE-2023-0286	7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H)	There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most

		cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.
CVE-2023-0394	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A NULL pointer dereference flaw was found in rawv6_push_pending_frames in net/ipv6/raw.c in the network subcomponent in the Linux kernel. This flaw causes the system to crash.
CVE-2023-0458	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)	A speculative pointer dereference problem exists in the Linux Kernel on the do_prlimit() function. The resource argument value is controlled and is used in pointer arithmetic for the 'rlim' variable and can be used to leak the contents. We recommend upgrading past version 6.1.8 or commit 739790605705ddcf18f21782b9c99ad7d53a8c11
CVE-2023-0461	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	There is a use-after-free vulnerability in the Linux Kernel which can be exploited to achieve local privilege escalation. To reach the vulnerability kernel configuration flag CONFIG_TLS or CONFIG_XFRM_ESPINTCP has to be configured, but the operation does not require any privilege. There is a use-after-free bug of icsk_ulp_data of a struct inet_connection_sock. When CONFIG_TLS is enabled, user can install a tls context (struct tls_context) on a connected tcp socket. The context is not cleared if this socket is disconnected and reused as a listener. If a new socket is created from the listener, the context is inherited and vulnerable. The setsockopt TCP_ULP operation does not require any

		privilege. We recommend upgrading past commit 2c02d41d71f90a5168391b6a5f2954112ba2307c
CVE-2023-0590	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)	A use-after-free flaw was found in qdisc_graft in net/sched/sch_api.c in the Linux Kernel due to a race problem. This flaw leads to a denial of service issue. If patch ebda44da44f6 ("net: sched: fix race condition in qdisc_graft()") not applied yet, then kernel could be affected.
CVE-2023-0597	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)	A flaw possibility of memory leak in the Linux kernel cpu_entry_area mapping of X86 CPU data to memory was found in the way user can guess location of exception stack(s) or other important data. A local user could use this flaw to get access to some important data with expected location in memory.
CVE-2023-0767	8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	An attacker could construct a PKCS 12 cert bundle in such a way that could allow for arbitrary memory writes via PKCS 12 Safe Bag attributes being mishandled. This vulnerability affects Firefox < 110, Thunderbird < 102.8, and Firefox ESR < 102.8.
CVE-2023-1073	6.6 (CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A memory corruption flaw was found in the Linux kernel's human interface device (HID) subsystem in how a user inserts a malicious USB device. This flaw allows a local user to crash or potentially escalate their privileges on the system.
CVE-2023-1074	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A memory leak flaw was found in the Linux kernel's Stream Control Transmission Protocol. This issue may occur when a user starts a malicious networking service and someone connects to this service. This could allow a local user to starve resources, causing a denial of service.

CVE-2023-1075	3.3 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)	A flaw was found in the Linux Kernel. The tls_is_tx_ready() incorrectly checks for list emptiness, potentially accessing a type confused entry to the list_head, leaking the last byte of the confused field that overlaps with rec->tx_ready.
CVE-2023-1079	6.8 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	A flaw was found in the Linux kernel. A use-after-free may be triggered in asus_kbd_backlight_set when plugging/disconnecting in a malicious USB device, which advertises itself as an Asus device. Similarly to the previous known CVE-2023-25012, but in asus devices, the work_struct may be scheduled by the LED controller while the device is disconnecting, triggering a use-after-free on the struct asus_kbd_leds *led structure. A malicious USB device may exploit the issue to cause memory corruption with controlled data.
CVE-2023-1118	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A flaw use after free in the Linux kernel integrated infrared receiver/transceiver driver was found in the way user detaching rc device. A local user could use this flaw to crash the system or potentially escalate their privileges on the system.
CVE-2023-1192	6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A use-after-free flaw was found in smb2_is_status_io_timeout() in CIFS in the Linux Kernel. After CIFS transfers response data to a system call, there are still local variable points to the memory region, and if the system call frees it faster than CIFS uses it, CIFS will access a free memory region, leading to a denial of service.
CVE-2023-	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A use-after-free flaw was found in reconn_set_ipaddr_from_hostname in fs/cifs/connect.c in the Linux kernel. The issue occurs when it forgets to set

1195		the free pointer server->hostname to NULL, leading to an invalid pointer request.
CVE-2023-1206	5.7 (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A hash collision flaw was found in the IPv6 connection lookup table in the Linux kernel's IPv6 functionality when a user makes a new kind of SYN flood attack. A user located in the local network or with a high bandwidth connection can increase the CPU usage of the server that accepts IPV6 connections up to 95%.
CVE-2023-1252	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A use-after-free flaw was found in the Linux kernel's Ext4 File System in how a user triggers several file operations simultaneously with the overlay FS usage. This flaw allows a local user to crash or potentially escalate their privileges on the system. Only if patch 9a2544037600 ("ovl: fix use after free in struct ovl_aio_req") not applied yet, the kernel could be affected.
CVE-2023-1281	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	Use After Free vulnerability in Linux kernel traffic control index filter (tcindex) allows Privilege Escalation. The imperfect hash area can be updated while packets are traversing, which will cause a use-after-free when 'tcf_exts_exec()' is called with the destroyed tcf_ext. A local attacker user can use this vulnerability to elevate its privileges to root. This issue affects Linux Kernel: from 4.14 before git commit ee059170b1f7e94e55fa6cadee544e176a6e59c2.
CVE-2023-1382	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)	A data race flaw was found in the Linux kernel, between where con is allocated and con->sock is set. This issue leads to a NULL pointer dereference when accessing con->sock->sk in net/tipc/topsrv.c in the tipc protocol in the Linux kernel.

CVE-2023-1582	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)	A race problem was found in fs/proc/task_mmu.c in the memory management sub-component in the Linux kernel. This issue may allow a local attacker with user privilege to cause a denial of service.
CVE-2023-1829	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A use-after-free vulnerability in the Linux Kernel traffic control index filter (tcindex) can be exploited to achieve local privilege escalation. The tcindex_delete function which does not properly deactivate filters in case of a perfect hashes while deleting the underlying structure which can later lead to double freeing the structure. A local attacker user can use this vulnerability to elevate its privileges to root. We recommend upgrading past commit 8c710f75256bb3cf05ac7b1672c82b92c43f3d28.
CVE-2023-1855	6.3 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H)	A use-after-free flaw was found in xgene_hwmon_remove in drivers/hwmon/xgene-hwmon.c in the Hardware Monitoring Linux Kernel Driver (xgene-hwmon). This flaw could allow a local attacker to crash the system due to a race problem. This vulnerability could even lead to a kernel information leak problem.
CVE-2023-1989	7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	A use-after-free flaw was found in btsdio_remove in drivers\bluetooth\btsdio.c in the Linux Kernel. In this flaw, a call to btsdio_remove with an unfinished job, may cause a race problem leading to a UAF on hdev devices.
CVE-2023-1998	5.6 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N)	The Linux kernel allows userspace processes to enable mitigations by calling prctl with PR_SET_SPECULATION_CTRL which disables the speculation feature as well as by using seccomp. We had noticed that on VMs of at least one major cloud provider, the kernel still left the victim process exposed to attacks in

		some cases even after enabling the spectre-BTI mitigation with prctl. The same behavior can be observed on a bare-metal machine when forcing the mitigation to IBRS on boot command line. This happened because when plain IBRS was enabled (not enhanced IBRS), the kernel had some logic that determined that STIBP was not needed. The IBRS bit implicitly protects against cross-thread branch target injection. However, with legacy IBRS, the IBRS bit was cleared on returning to userspace, due to performance reasons, which disabled the implicit STIBP and left userspace threads vulnerable to cross-thread branch target injection against which STIBP protects.
CVE-2023-20569	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)	A side channel vulnerability on some of the AMD CPUs may allow an attacker to influence the return address prediction. This may result in speculative execution at an attacker-controlled address, potentially leading to information disclosure.
CVE-2023-20593	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)	An issue in “Zen 2” CPUs, under specific microarchitectural circumstances, may allow an attacker to potentially access sensitive information.
CVE-2023-2124	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	An out-of-bounds memory access flaw was found in the Linux kernel’s XFS file system in how a user restores an XFS image after failure (with a dirty log journal). This flaw allows a local user to crash or potentially escalate their privileges on the system.

CVE-2023-2163	8.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)	Incorrect verifier pruning in BPF in Linux Kernel >=5.4 leads to unsafe code paths being incorrectly marked as safe, resulting in arbitrary read/write in kernel memory, lateral privilege escalation, and container escape.
CVE-2023-2176	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A vulnerability was found in compare_netdev_and_ip in drivers/infiniband/core/cma.c in RDMA in the Linux Kernel. The improper cleanup results in out-of-boundary read, where a local user can utilize this problem to crash the system or escalation of privilege.
CVE-2023-21930	7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.4

		(Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).
CVE-2023-21937	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2023-21938	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 and 22.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java

		deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2023-21939	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2023-	6.7 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	An out-of-bounds write vulnerability was found in the Linux kernel's SLIMpro I2C device driver. The userspace "data->block[0]" variable was not capped to a number between 0-255 and was used as the size of a memcpy, possibly writing beyond the end of dma_buffer. This flaw

2194		could allow a local privileged user to crash the system or potentially achieve code execution.
CVE-2023-21954	5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2023-21967	5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability

		applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2023-21968	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u361, 8u361-perf, 11.0.18, 17.0.6, 20; Oracle GraalVM Enterprise Edition: 20.3.9, 21.3.5 and 22.3.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2023-22	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition:

045		20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2023-22049	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7 and 20.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start

		applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2023-22081	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u381, 8u381-perf, 11.0.20, 17.0.8, 21; Oracle GraalVM for JDK: 17.0.8, 21; Oracle GraalVM Enterprise Edition: 20.3.11, 21.3.7 and 22.3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2023-2235	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A use-after-free vulnerability in the Linux Kernel Performance Events system can be exploited to achieve local privilege escalation. The perf_group_detach function did not check the event's siblings' attach_state before calling add_event_to_groups(), but remove_on_exec made it possible to call list_del_event() on before detaching from their group, making it possible to use a

		dangling pointer causing a use-after-free vulnerability. We recommend upgrading past commit fd0815f632c24878e325821943edccc7fde947a2.
CVE-2023-23454	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	cbq_classify in net/sched/sch_cbq.c in the Linux kernel through 6.1.4 allows attackers to cause a denial of service (slab-out-of-bounds read) because of type confusion (non-negative numbers can sometimes indicate a TC_ACT_SHOT condition rather than valid classification results).
CVE-2023-23455	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	atm_tc_enqueue in net/sched/sch_atm.c in the Linux kernel through 6.1.4 allows attackers to cause a denial of service because of type confusion (non-negative numbers can sometimes indicate a TC_ACT_SHOT condition rather than valid classification results).
CVE-2023-23918	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	A privilege escalation vulnerability exists in Node.js <19.6.1, <18.14.1, <16.19.1 and <14.21.3 that made it possible to bypass the experimental Permissions (https://nodejs.org/api/permissions.html) feature in Node.js and access non authorized modules by using process.mainModule.require(). This only affects users who had enabled the experimental permissions option with --experimental-policy.
CVE-2023-23920	4.2 (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N)	An untrusted search path vulnerability exists in Node.js. <19.6.1, <18.14.1, <16.19.1, and <14.21.3 that could allow an attacker to search and potentially load ICU data when running with elevated privileges.

CVE-2023-2432 9	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)	An issue in the urllib.parse component of Python before 3.11.4 allows attackers to bypass blocklisting methods by supplying a URL that starts with blank characters.
CVE-2023-2513	6.7 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	A use-after-free vulnerability was found in the Linux kernel's ext4 filesystem in the way it handled the extra inode size for extended attributes. This flaw could allow a privileged local user to cause a system crash or other undefined behaviors.
CVE-2023-2650	6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)	Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that use OBJ_obj2txt() directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit may experience notable to very long delays when processing those messages, which may lead to a Denial of Service. An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers - most of which have no size limit. OBJ_obj2txt() may be used to translate an ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSL type ASN1_OBJECT) to its canonical numeric text form, which are the sub-identifiers of the OBJECT IDENTIFIER in decimal form, separated by periods. When one of the sub-identifiers in the OBJECT IDENTIFIER is very large (these are sizes that are seen as absurdly large, taking up tens or hundreds of KiBs), the translation to a decimal number in text may take a very long time. The time complexity is O(n^2) with 'n' being the size of the sub-identifiers in bytes (*). With OpenSSL 3.0, support to fetch cryptographic algorithms using names / identifiers in string form was introduced.

		This includes using OBJECT IDENTIFIERs in canonical numeric text form as identifiers for fetching algorithms. Such OBJECT IDENTIFIERs may be received through the ASN.1 structure AlgorithmIdentifier, which is commonly used in multiple protocols to specify what cryptographic algorithm should be used to sign or verify, encrypt or decrypt, or digest passed data. Applications that call OBJ_obj2txt() directly with untrusted data are affected, with any version of OpenSSL. If the use is for the mere purpose of display, the severity is considered low. In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS. It also impacts anything that processes X.509 certificates, including simple things like verifying its signature. The impact on TLS is relatively low, because all versions of OpenSSL have a 100KiB limit on the peer's certificate chain. Additionally, this only impacts clients, or servers that have explicitly enabled client authentication. In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects, such as X.509 certificates. This is assumed to not happen in such a way that it would cause a Denial of Service, so these versions are considered not affected by this issue in such a way that it would be cause for concern, and the severity is therefore considered low.
CVE-2023-26545	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel before 6.1.13, there is a double free in net/mpls/af_mpls.c upon an allocation failure (for registering the sysctl table under a new location) during the renaming of a device.
CVE-2023-	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	systemd before 247 does not adequately block local privilege escalation for some Sudo configurations, e.g., plausible sudoers files in which the "systemctl status" command may be executed. Specifically, systemd does not

26604		set LESSSECURE to 1, and thus other programs may be launched from the less program. This presents a substantial security risk when running systemctl from Sudo, because less executes as root when the terminal size is too small to show the complete systemctl output.
CVE-2023-26916	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)	libyang from v2.0.164 to v2.1.30 was discovered to contain a NULL pointer dereference via the function lys_parse_mem at lys_parse_mem.c.
CVE-2023-2828	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	Every `named` instance configured to run as a recursive resolver maintains a cache database holding the responses to the queries it has recently sent to authoritative servers. The size limit for that cache database can be configured using the `max-cache-size` statement in the configuration file; it defaults to 90% of the total amount of memory available on the host. When the size of the cache reaches 7/8 of the configured limit, a cache-cleaning algorithm starts to remove expired and/or least-recently used RRsets from the cache, to keep memory use below the configured limit. It has been discovered that the effectiveness of the cache-cleaning algorithm used in `named` can be severely diminished by querying the resolver for specific RRsets in a certain order, effectively allowing the configured `max-cache-size` limit to be significantly exceeded. This issue affects BIND 9 versions 9.11.0 through 9.16.41, 9.18.0 through 9.18.15, 9.19.0 through 9.19.13, 9.11.3-S1 through 9.16.41-S1, and 9.18.11-S1 through 9.18.15-S1.
CVE-20	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A NULL pointer dereference flaw was found in the az6027 driver in drivers/media/usb/dev-usb/az6027.c in the Linux Kernel. The message from user space is not checked

23-28328		properly before transferring into the device. This flaw allows a local user to crash the system or potentially cause a denial of service.
CVE-2023-28746	6.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)	Information exposure through microarchitectural state after transient execution from some register files for some Intel(R) Atom(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2023-28772	6.7 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	An issue was discovered in the Linux kernel before 5.13.3. lib/seq_buf.c has a seq_buf_putmem_hex buffer overflow.
CVE-2023-30456	6.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H)	An issue was discovered in arch/x86/kvm/vmx/nested.c in the Linux kernel before 6.2.8. nVMX on x86_64 lacks consistency checks for CR0 and CR4.
CVE-2023-31084	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	An issue was discovered in drivers/media/dvb-core/dvb_frontend.c in the Linux kernel 6.2. There is a blocking operation when a task is in !TASK_RUNNING. In dvb_frontend_get_event, wait_event_interruptible is called; the condition is dvb_frontend_test_event(fepriv,events). In dvb_frontend_test_event, down(&fepriv->sem) is called.

		However, wait_event_interruptible would put the process to sleep, and down(&fepriv->sem) may block the process.
CVE-2023-3141	7.1 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)	A use-after-free flaw was found in r592_remove in drivers/memstick/host/r592.c in media access in the Linux Kernel. This flaw allows a local attacker to crash the system at device disconnect, possibly leading to a kernel information leak.
CVE-2023-3143 6	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	qfq_change_class in net/sched/sch_qfq.c in the Linux kernel before 6.2.13 allows an out-of-bounds write because lmax can exceed QFQ_MIN_LMAX.
CVE-2023-3161	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A flaw was found in the Framebuffer Console (fbcon) in the Linux Kernel. When providing font->width and font->height greater than 32 to fbcon_set_font, since there are no checks in place, a shift-out-of-bounds occurs leading to undefined behavior and possible denial of service.
CVE-2023-3206 7	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	c-ares is an asynchronous resolver library. c-ares is vulnerable to denial of service. If a target resolver sends a query, the attacker forges a malformed UDP packet with a length of 0 and returns them to the target resolver. The target resolver erroneously interprets the 0 length as a graceful shutdown of the connection. This issue has been patched in version 1.19.1.
CVE-2023-	4.4 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H)	A NULL pointer dereference issue was found in the gfs2 file system in the Linux kernel. It occurs on corrupt gfs2 file systems when the evict code tries to reference the journal descriptor structure after it has been freed and set

3212		to NULL. A privileged local user could use this flaw to cause a kernel panic.
CVE-2023-32360	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N)	An authentication issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13.4. An unauthenticated user may be able to access recently printed documents.
CVE-2023-3268	7.1 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)	An out of bounds (OOB) memory access flaw was found in the Linux kernel in relay_file_read_start_pos in kernel/relay.c in the relayfs. This flaw could allow a local attacker to crash the system or leak kernel internal information.
CVE-2023-33203	6.4 (CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/net/ethernet/qualcomm/emac/emac.c if a physically proximate attacker unplugs an emac based device.
CVE-2023-33341	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	The code that processes control channel messages sent to `named` calls certain functions recursively during packet parsing. Recursion depth is only limited by the maximum accepted packet size; depending on the environment, this may cause the packet-parsing code to run out of available stack memory, causing `named` to terminate unexpectedly. Since each incoming control channel message is fully parsed before its contents are authenticated, exploiting this flaw does not require the attacker to hold a valid RNDC key; only network access to the control channel's configured TCP port is necessary.

		This issue affects BIND 9 versions 9.2.0 through 9.16.43, 9.18.0 through 9.18.18, 9.19.0 through 9.19.16, 9.9.3-S1 through 9.16.43-S1, and 9.18.0-S1 through 9.18.18-S1.
CVE-2023-33951	5.3 (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N)	A race condition vulnerability was found in the vmwgfx driver in the Linux kernel. The flaw exists within the handling of GEM objects. The issue results from improper locking when performing operations on an object. This flaw allows a local privileged user to disclose information in the context of the kernel.
CVE-2023-33952	6.7 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	A double-free vulnerability was found in handling vmw_buffer_object objects in the vmwgfx driver in the Linux kernel. This issue occurs due to the lack of validating the existence of an object prior to performing further free operations on the object, which may allow a local privileged user to escalate privileges and execute code in the context of the kernel.
CVE-2023-3446	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a

		key or parameters obtained from an untrusted source could be vulernable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.
CVE-2023-35823	7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in saa7134_finidev in drivers/media/pci/saa7134/saa7134-core.c.
CVE-2023-35824	7.0 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in dm1105_remove in drivers/media/pci/dm1105/dm1105.c.
CVE-2023-35825		Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-3141. Reason: This candidate is a reservation duplicate of CVE-2023-3141. Notes: All CVE users should reference CVE-2023-3141 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.

CVE-2023-3609	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A use-after-free vulnerability in the Linux kernel's net/sched: cls_u32 component can be exploited to achieve local privilege escalation. If tcf_change_indev() fails, u32_set_parms() will immediately return an error after incrementing or decrementing the reference counter in tcf_bind_filter(). If an attacker can control the reference counter and set it to zero, they can cause the reference to be freed, leading to a use-after-free vulnerability. We recommend upgrading past commit 04c55383fa5689357bcdd2c8036725a55ed632bc.
CVE-2023-3611	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	An out-of-bounds write vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation. The qfq_change_agg() function in net/sched/sch_qfq.c allows an out-of-bounds write because lmax is updated according to packet sizes without bounds checks. We recommend upgrading past commit 3e337087c3b5805fe0b8a46ba622a962880b5d64.
CVE-2023-3772	4.4 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H)	A flaw was found in the Linux kernel’s IP framework for transforming packets (XFRM subsystem). This issue may allow a malicious user with CAP_NET_ADMIN privileges to directly dereference a NULL pointer in xfrm_update_ae_params(), leading to a possible kernel crash and denial of service.
CVE-2023-3812	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	An out-of-bounds memory access flaw was found in the Linux kernel’s TUN/TAP device driver functionality in how a user generates a malicious (too big) networking packet when napi frags is enabled. This flaw allows a local user to crash or potentially escalate their privileges on the system.
CVE-2023-	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a

3817		DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the "-check" option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.
CVE-2023-38408	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.
CVE-2023-38	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	FRRouting FRR 7.5.1 through 9.0 and Pica8 PICOS 4.3.3.2 allow a remote attacker to cause a denial of service via a crafted BGP update with a corrupted attribute 23 (Tunnel Encapsulation).

802		
CVE-2023-4021 7	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)	An issue was discovered in Python before 3.8.18, 3.9.x before 3.9.18, 3.10.x before 3.10.13, and 3.11.x before 3.11.5. It primarily affects servers (such as HTTP servers) that use TLS client authentication. If a TLS server-side socket is created, receives data into the socket buffer, and then is closed quickly, there is a brief window where the SSLSocket instance will detect the socket as "not connected" and won't initiate a handshake, but buffered data will still be readable from the socket buffer. This data will not be authenticated if the server-side TLS peer is expecting client certificate authentication, and is indistinguishable from valid TLS stream data. Data is limited in size to the amount that will fit in the buffer. (The TLS connection cannot directly be used for data exfiltration because the vulnerable code path requires that the connection be closed on initialization of the SSLSocket.)
CVE-2023-4028 3	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	An issue was discovered in l2cap_sock_release in net/bluetooth/l2cap_sock.c in the Linux kernel before 6.4.10. There is a use-after-free because the children of an sk are mishandled.
CVE-2023-4128		Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-4206, CVE-2023-4207, CVE-2023-4208. Reason: This record is a duplicate of CVE-2023-4206, CVE-2023-4207, CVE-2023-4208. Notes: All CVE users should reference CVE-2023-4206, CVE-2023-4207, CVE-2023-4208 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.

CVE-2023-4132	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	A use-after-free vulnerability was found in the siano smsusb module in the Linux kernel. The bug occurs during device initialization when the siano device is plugged in. This flaw allows a local user to crash the system, causing a denial of service condition.
CVE-2023-4155	5.6 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:N/I:N/A:H)	A flaw was found in KVM AMD Secure Encrypted Virtualization (SEV) in the Linux kernel. A KVM guest using SEV-ES or SEV-SNP with multiple vCPUs can trigger a double fetch race condition vulnerability and invoke the `VMGEXIT` handler recursively. If an attacker manages to call the handler multiple times, they can trigger a stack overflow and cause a denial of service or potentially guest-to-host escape in kernel configurations without stack guard pages (`CONFIG_VMAP_STACK`).
CVE-2023-4206	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A use-after-free vulnerability in the Linux kernel's net/sched: cls_route component can be exploited to achieve local privilege escalation. When route4_change() is called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This causes a problem when updating a filter bound to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the still referenced class and allowing it to be deleted, leading to a use-after-free. We recommend upgrading past commit b80b829e9e2c1b3f7aae34855e04d8f6ecaf13c8.
CVE-2023-4207	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A use-after-free vulnerability in the Linux kernel's net/sched: cls_fw component can be exploited to achieve local privilege escalation. When fw_change() is called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This causes a problem when updating a filter bound to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the still

		referenced class and allowing it to be deleted, leading to a use-after-free. We recommend upgrading past commit 76e42ae831991c828cffa8c37736ebfb831ad5ec.
CVE-2023-4208	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A use-after-free vulnerability in the Linux kernel's net/sched: cls_u32 component can be exploited to achieve local privilege escalation. When u32_change() is called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This causes a problem when updating a filter bound to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the still referenced class and allowing it to be deleted, leading to a use-after-free. We recommend upgrading past commit 3044b16e7c6fe5d24b1cdbcf1bd0a9d92d1ebd81.
CVE-2023-4408	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	The DNS message parsing code in `named` includes a section whose computational complexity is overly high. It does not cause problems for typical DNS traffic, but crafted queries and responses may cause excessive CPU load on the affected `named` instance by exploiting this flaw. This issue affects both authoritative servers and recursive resolvers. This issue affects BIND 9 versions 9.0.0 through 9.16.45, 9.18.0 through 9.18.21, 9.19.0 through 9.19.19, 9.9.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.45-S1, and 9.18.11-S1 through 9.18.21-S1.
CVE-2023-4623	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A use-after-free vulnerability in the Linux kernel's net/sched: sch_hfsc (HFSC qdisc traffic control) component can be exploited to achieve local privilege escalation. If a class with a link-sharing curve (i.e. with the HFSC_FSC flag set) has a parent without a link-sharing curve, then init_vf() will call vttree_insert() on the parent, but vttree_remove() will be skipped in update_vf(). This leaves a dangling pointer that can cause a use-after-free. We recommend upgrading past commit b3d26c5702c7d6c45456326e56d2ccf3f103e60f.

CVE-2023-46724	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	Squid is a caching proxy for the Web. Due to an Improper Validation of Specified Index bug, Squid versions 3.3.0.1 through 5.9 and 6.0 prior to 6.4 compiled using `--with-openssl` are vulnerable to a Denial of Service attack against SSL Certificate validation. This problem allows a remote server to perform Denial of Service against Squid Proxy by initiating a TLS Handshake with a specially crafted SSL Certificate in a server certificate chain. This attack is limited to HTTPS and SSL-Bump. This bug is fixed in Squid version 6.4. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives. Those who you use a prepackaged version of Squid should refer to the package vendor for availability information on updated packages.
CVE-2023-46728	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to a NULL pointer dereference bug Squid is vulnerable to a Denial of Service attack against Squid's Gopher gateway. The gopher protocol is always available and enabled in Squid prior to Squid 6.0.1. Responses triggering this bug are possible to be received from any gopher server, even those without malicious intent. Gopher support has been removed in Squid version 6.0.1. Users are advised to upgrade. Users unable to upgrade should reject all gopher URL requests.
CVE-2023-46846	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)	SQUID is vulnerable to HTTP request smuggling, caused by chunked decoder lenience, allows a remote attacker to perform Request/Response smuggling past firewall and frontend security systems.
CVE-20	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	Squid is vulnerable to a Denial of Service, where a remote attacker can perform buffer overflow attack by writing up

23-46847		to 2 MB of arbitrary data to heap memory when Squid is configured to accept HTTP Digest Authentication.
CVE-2023-47132	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)	A flaw was found in pfn_swap_entry_to_page in memory management subsystem in the Linux Kernel. In this flaw, an attacker with a local user privilege may cause a denial of service problem due to a BUG statement referencing pmd_t x.
CVE-2023-481611	7.1 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)	Buffer Overflow vulnerability in GifLib Project GifLib v.5.2.1 allows a local attacker to obtain sensitive information via the DumpSCreen2RGB function in gif2rgb.c
CVE-2023-48795	5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in

		Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.
CVE-2023-49285	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to a Buffer Overread bug Squid is vulnerable to a Denial of Service attack against Squid HTTP Message processing. This bug is fixed by Squid version 6.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.
CVE-2023-49286	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to an Incorrect Check of Function Return Value bug Squid is vulnerable to a Denial of Service attack against its Helper process management. This bug is fixed by Squid version 6.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.

CVE-2023-50269	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	Squid is a caching proxy for the Web. Due to an Uncontrolled Recursion bug in versions 2.6 through 2.7.STABLE9, versions 3.1 through 5.9, and versions 6.0.1 through 6.5, Squid may be vulnerable to a Denial of Service attack against HTTP Request parsing. This problem allows a remote client to perform Denial of Service attack by sending a large X-Forwarded-For header when the follow_x_forwarded_for feature is configured. This bug is fixed by Squid version 6.6. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives.
CVE-2023-50387	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.
CVE-2023-50868	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.
CVE-2023-51078	8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A use-after-free vulnerability was found in drivers/nvme/target/tcp.c` in `nvmet_tcp_free_crypto` due to a logical bug in the NVMe/TCP subsystem in the Linux kernel. This issue may allow a malicious user to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation.

CVE-2023-52451	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/memhp: Fix access beyond end of drmem array dlpar_memory_remove_by_index() may access beyond the bounds of the drmem lmb array when the LMB lookup fails to match an entry with the given DRC index. When the search fails, the cursor is left pointing to &drmem_info->lmbs[drmem_info->n_lmbs], which is one element past the last valid entry in the array. The debug message at the end of the function then dereferences this pointer: pr_debug("Failed to hot-remove memory at %llx\n", lmb->base_addr); This was found by inspection and confirmed with KASAN: pseries-hotplug-mem: Attempting to hot-remove LMB, drc index 1234 == BUG: KASAN: slab-out-of-bounds in dlpar_memory+0x298/0x1658 Read of size 8 at addr c000000364e97fd0 by task bash/949 dump_stack_lvl+0xa4/0xfc (unreliable) print_report+0x214/0x63c kasan_report+0x140/0x2e0 __asan_load8+0xa8/0xe0 dlpar_memory+0x298/0x1658 handle_dlpar_errorlog+0x130/0x1d0 dlpar_store+0x18c/0x3e0 kobj_attr_store+0x68/0xa0 sysfs_kf_write+0xc4/0x110 kernfs_fop_write_iter+0x26c/0x390 vfs_write+0x2d4/0x4e0 ksys_write+0xac/0x1a0 system_call_exception+0x268/0x530 system_call_vectored_common+0x15c/0x2ec Allocated by task 1: kasan_save_stack+0x48/0x80 kasan_set_track+0x34/0x50 kasan_save_alloc_info+0x34/0x50 __kasan_kmalloc+0xd0/0x120 __kmalloc+0x8c/0x320 kmalloc_array.constprop.0+0x48/0x5c drmem_init+0x2a0/0x41c do_one_initcall+0xe0/0x5c0 kernel_init_freeable+0x4ec/0x5a0 kernel_init+0x30/0x1e0 ret_from_kernel_user_thread+0x14/0x1c The buggy address belongs to the object at c000000364e80000 which belongs to the cache kmalloc-128k of size 131072

		The buggy address is located 0 bytes to the right of allocated 98256-byte region [c000000364e80000, c000000364e97fd0) ========== pseries-hotplug-mem: Failed to hot-remove memory at 0 Log failed lookups with a separate message and dereference the cursor only when it points to a valid entry.
CVE-2023-52463	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: efivarfs: force RO when remounting if SetVariable is not supported If SetVariable at runtime is not supported by the firmware we never assign a callback for that function. At the same time mount the efivarfs as RO so no one can call that. However, we never check the permission flags when someone remounts the filesystem as RW. As a result this leads to a crash looking like this: $ mount -o remount,rw /sys/firmware/efi/efivars $ efi-updatevar -f PK.auth PK [303.279166] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 [303.280482] Mem abort info: [303.280854] ESR = 0x0000000086000004 [303.281338] EC = 0x21: IABT (current EL), IL = 32 bits [303.282016] SET = 0, FnV = 0 [303.282414] EA = 0, S1PTW = 0 [303.282821] FSC = 0x04: level 0 translation fault [303.283771] user pgtable: 4k pages, 48-bit VAs, pgdp=000000004258c000 [303.284913] [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 [303.286076] Internal error: Oops: 0000000086000004 [#1] PREEMPT SMP [303.286936] Modules linked in: qrtr tpm_tis tpm_tis_core crct10dif_ce arm_smccc_trng rng_core drm fuse ip_tables x_tables ipv6 [303.288586] CPU: 1 PID: 755 Comm: efi-updatevar Not tainted 6.3.0-rc1-00108-gc7d0c4695c68 #1 [303.289748] Hardware name: Unknown Unknown Product/Unknown Product, BIOS 2023.04-00627-g88336918701d 04/01/2023 [303.291150] pstate:

		60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [303.292123] pc : 0x0 [303.292443] lr : efivar_set_variable_locked+0x74/0xec [303.293156] sp : ffff800008673c10 [303.293619] x29: ffff800008673c10 x28: ffff0000037e8000 x27: 0000000000000000 [303.294592] x26: 0000000000000800 x25: ffff000002467400 x24: 0000000000000027 [303.295572] x23: ffffd49ea9832000 x22: ffff0000020c9800 x21: ffff000002467000 [303.296566] x20: 0000000000000001 x19: 00000000000007fc x18: 0000000000000000 [303.297531] x17: 0000000000000000 x16: 0000000000000000 x15: 0000aaaac807ab54 [303.298495] x14: ed37489f673633c0 x13: 71c45c606de13f80 x12: 47464259e219acf4 [303.299453] x11: ffff000002af7b01 x10: 0000000000000003 x9 : 0000000000000002 [303.300431] x8 : 0000000000000010 x7 : ffffd49ea8973230 x6 : 0000000000a85201 [303.301412] x5 : 0000000000000000 x4 : ffff0000020c9800 x3 : 00000000000007fc [303.302370] x2 : 0000000000000027 x1 : ffff000002467400 x0 : ffff000002467000 [303.303341] Call trace: [303.303679] 0x0 [303.303938] efivar_entry_set_get_size+0x98/0x16c [303.304585] efivarfs_file_write+0xd0/0x1a4 [303.305148] vfs_write+0xc4/0x2e4 [303.305601] ksys_write+0x70/0x104 [303.306073] __arm64_sys_write+0x1c/0x28 [303.306622] invoke_syscall+0x48/0x114 [303.307156] el0_svc_common.constprop.0+0x44/0xec [303.307803] do_el0_svc+0x38/0x98 [303.308268] el0_svc+0x2c/0x84 [303.308702] el0t_64_sync_handler+0xf4/0x120 [303.309293] el0t_64_sync+0x190/0x194 [303.309794] Code: ???????? ???????? ???????? ???????? (????????) [303.310612] ---[end trace 0000000000000000]--- Fix this by adding a .reconfigure() function to the fs operations which we can use to check the requested flags and deny

		anything that's not RO if the firmware doesn't implement SetVariable at runtime.
CVE-2023-52469	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: drivers/amd/pm: fix a use-after-free in kv_parse_power_table When ps allocated by kzalloc equals to NULL, kv_parse_power_table frees adev->pm.dpm.ps that allocated before. However, after the control flow goes through the following call chains: kv_parse_power_table |-> kv_dpm_init |-> kv_dpm_sw_init |-> kv_dpm_fini The adev->pm.dpm.ps is used in the for loop of kv_dpm_fini after its first free in kv_parse_power_table and causes a use-after-free bug.
CVE-2023-52471	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: ice: Fix some null pointer dereference issues in ice_ptp.c devm_kasprintf() returns a pointer to dynamically allocated memory which can be NULL upon failure.
CVE-2023-52486	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: drm: Don't unref the same fb many times by mistake due to deadlock handling If we get a deadlock after the fb lookup in drm_mode_page_flip_ioctl() we proceed to unref the fb and then retry the whole thing from the top. But we forget to reset the fb pointer back to NULL, and so if we then get another error during the retry, before the fb lookup, we proceed the unref the same fb again without having gotten another reference. The end result is that the fb will (eventually) end up being freed while it's still in use. Reset fb to NULL once we've unreffed it to avoid doing it again until we've done another fb lookup. This turned out to be pretty easy to hit on a DG2 when doing async flips (and CONFIG_DEBUG_WW_MUTEX_SLOWPATH=y). The first

		symptom I saw that drm_closefb() simply got stuck in a busy loop while walking the framebuffer list. Fortunately I was able to convince it to oops instead, and from there it was easier to track down the culprit.
CVE-2023-52530	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix potential key use-after-free When ieee80211_key_link() is called by ieee80211_gtk_rekey_add() but returns 0 due to KRACK protection (identical key reinstall), ieee80211_gtk_rekey_add() will still return a pointer into the key, in a potential use-after-free. This normally doesn't happen since it's only called by iwlwifi in case of WoWLAN rekey offload which has its own KRACK protection, but still better to fix, do that by returning an error code and converting that to success on the cfg80211 boundary only, leaving the error for bad callers of ieee80211_gtk_rekey_add().
CVE-2023-52619	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: pstore/ram: Fix crash when setting number of cpus to an odd number When the number of cpu cores is adjusted to 7 or other odd numbers, the zone size will become an odd number. The address of the zone will become: addr of zone0 = BASE addr of zone1 = BASE + zone_size addr of zone2 = BASE + zone_size*2 ... The address of zone1/3/5/7 will be mapped to non-alignment va. Eventually crashes will occur when accessing these va. So, use ALIGN_DOWN() to make sure the zone size is even to avoid this bug.
CVE-2023-52	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: ext4: avoid online resizing failures due to oversized flex bg When we online resize an ext4 filesystem with a oversized flexbg_size, mkfs.ext4 -F -G 67108864 $dev -b 4096 100M mount $dev $dir resize2fs $dev 16G the following WARN_ON is triggered:

622		========== WARNING: CPU: 0 PID: 427 at mm/page_alloc.c:4402 __alloc_pages+0x411/0x550 Modules linked in: sg(E) CPU: 0 PID: 427 Comm: resize2fs Tainted: G E 6.6.0-rc5+ #314 RIP: 0010:__alloc_pages+0x411/0x550 Call Trace: <TASK> __kmalloc_large_node+0xa2/0x200 __kmalloc+0x16e/0x290 ext4_resize_fs+0x481/0xd80 __ext4_ioctl+0x1616/0x1d90 ext4_ioctl+0x12/0x20 __x64_sys_ioctl+0xf0/0x150 do_syscall_64+0x3b/0x90 ========== This is because flexbg_size is too large and the size of the new_group_data array to be allocated exceeds MAX_ORDER. Currently, the minimum value of MAX_ORDER is 8, the minimum value of PAGE_SIZE is 4096, the corresponding maximum number of groups that can be allocated is: (PAGE_SIZE << MAX_ORDER) / sizeof(struct ext4_new_group_data) ≈ 21845 And the value that is down-aligned to the power of 2 is 16384. Therefore, this value is defined as MAX_RESIZE_BG, and the number of groups added each time does not exceed this value during resizing, and is added multiple times to complete the online resizing. The difference is that the metadata in a flex_bg may be more dispersed.
CVE-2023-52623	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: Fix a suspicious RCU usage warning I received the following warning while running cthon against an ontap server running pNFS: [57.202521] ========== [57.202522] WARNING: suspicious RCU usage [57.202523] 6.7.0-rc3-g2cc14f52aeb7 #41492 Not tainted [57.202525] ---------- [57.202525] net/sunrpc/xprtmultipath.c:349 RCU-list traversed in non-reader section!! [57.202527] other info that might help us debug this: [57.202528] rcu_scheduler_active = 2, debug_locks = 1 [57.202529] no

		locks held by test5/3567. [57.202530] stack backtrace: [57.202532] CPU: 0 PID: 3567 Comm: test5 Not tainted 6.7.0-rc3-g2cc14f52aeb7 #41492 5b09971b4965c0aceba19f3eea324a4a806e227e [57.202534] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS unknown 2/2/2022 [57.202536] Call Trace: [57.202537] <TASK> [57.202540] dump_stack_lvl+0x77/0xb0 [57.202551] lockdep_rcu_suspicious+0x154/0x1a0 [57.202556] rpc_xprt_switch_has_addr+0x17c/0x190 [sunrpc ebe02571b9a8ceebf7d98e71675af20c19bdb1f6] [57.202596] rpc_clnt_setup_test_and_add_xprt+0x50/0x180 [sunrpc ebe02571b9a8ceebf7d98e71675af20c19bdb1f6] [57.202621] ? rpc_clnt_add_xprt+0x254/0x300 [sunrpc ebe02571b9a8ceebf7d98e71675af20c19bdb1f6] [57.202646] rpc_clnt_add_xprt+0x27a/0x300 [sunrpc ebe02571b9a8ceebf7d98e71675af20c19bdb1f6] [57.202671] ? __pfx_rpc_clnt_setup_test_and_add_xprt+0x10/0x10 [sunrpc ebe02571b9a8ceebf7d98e71675af20c19bdb1f6] [57.202696] nfs4_pnfs_ds_connect+0x345/0x760 [nfsv4 c716d88496ded0ea6d289bbea684fa996f9b57a9] [57.202728] ? __pfx_nfs4_test_session_trunk+0x10/0x10 [nfsv4 c716d88496ded0ea6d289bbea684fa996f9b57a9] [57.202754] nfs4_fl_prepare_ds+0x75/0xc0 [nfs_layout_nfsv41_files e3a4187f18ae8a27b630f9feae6831b584a9360a] [57.202760] filelayout_write_pagelist+0x4a/0x200 [nfs_layout_nfsv41_files e3a4187f18ae8a27b630f9feae6831b584a9360a] [57.202765] pnfs_generic_pg_writepages+0xbe/0x230 [nfsv4 c716d88496ded0ea6d289bbea684fa996f9b57a9] [57.202788] __nfs_pageio_add_request+0x3fd/0x520 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202813] nfs_pageio_add_request+0x18b/0x390 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [

		57.202831] nfs_do_writepage+0x116/0x1e0 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202849] nfs_writepages_callback+0x13/0x30 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202866] write_cache_pages+0x265/0x450 [57.202870] ? __pfx_nfs_writepages_callback+0x10/0x10 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202891] nfs_writepages+0x141/0x230 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202913] do_writepages+0xd2/0x230 [57.202917] ? filemap_fdatawrite_wbc+0x5c/0x80 [57.202921] filemap_fdatawrite_wbc+0x67/0x80 [57.202924] filemap_write_and_wait_range+0xd9/0x170 [57.202930] nfs_wb_all+0x49/0x180 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202947] nfs4_file_flush+0x72/0xb0 [nfsv4 c716d88496ded0ea6d289bbea684fa996f9b57a9] [57.202969] __se_sys_close+0x46/0xd0 [57.202972] do_syscall_64+0x68/0x100 [57.202975] ? do_syscall_64+0x77/0x100 [57.202976] ? do_syscall_64+0x77/0x100 [57.202979] entry_SYSCALL_64_after_hwframe+0x6e/0x76 [57.202982] RIP: 0033:0x7fe2b12e4a94 [57.202985] Code: 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 80 3d d5 18 0e 00 00 74 13 b8 03 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 44 c3 0f 1f 00 48 83 ec 18 89 7c 24 0c e8 c3 [57.202987] RSP: 002b:00007ffe857ddb38 EFLAGS: 00000202 ORIG_RAX: 0000000000000003 [57.202989] RAX: ffffffffffffffda RBX: 00007ffe857dfd68 RCX: 00007fe2b12e4a94 [57.202991] RDX: 0000000000002000 RSI: 00007ffe857ddc40 RDI: 0000000000000003 [57.202992] RBP: 00007ffe857dfc50 R08: 7fffffffffffffff R09: 0000000065650f49 [57.202993] R10: 00007f ---truncated---

CVE-2023-52648	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Unmap the surface before resetting it on a plane state Switch to a new plane state requires unreferencing of all held surfaces. In the work required for mob cursors the mapped surfaces started being cached but the variable indicating whether the surface is currently mapped was not being reset. This leads to crashes as the duplicated state, incorrectly, indicates the that surface is mapped even when no surface is present. That's because after unreferencing the surface it's perfectly possible for the plane to be backed by a bo instead of a surface. Reset the surface mapped flag when unreferencing the plane state surface to fix null derefs in cleanup. Fixes crashes in KDE KWin 6.0 on Wayland: Oops: 0000 [#1] PREEMPT SMP PTI CPU: 4 PID: 2533 Comm: kwin_wayland Not tainted 6.7.0-rc3-vmwgfx #2 Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020 RIP: 0010:vmw_du_cursor_plane_cleanup_fb+0x124/0x140 [vmwgfx] Code: 00 00 00 75 3a 48 83 c4 10 5b 5d c3 cc cc cc cc 48 8b b3 a8 00 00 00 48 c7 c7 99 90 43 c0 e8 93 c5 db ca 48 8b 83 a8 00 00 00 <48> 8b 78 28 e8 e3 f> RSP: 0018:ffffb6b98216fa80 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff969d84cdcb00 RCX: 0000000000000027 RDX: 0000000000000000 RSI: 0000000000000001 RDI: ffff969e75f21600 RBP: ffff969d4143dc50 R08: 0000000000000000 R09: ffffb6b98216f920 R10: 0000000000000003 R11: ffff969e7feb3b10 R12: 0000000000000000 R13: 0000000000000000 R14: 000000000000027b R15: ffff969d49c9fc00 FS: 00007f1e8f1b4180(0000) GS:ffff969e75f00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000028 CR3: 0000000104006004 CR4: 00000000003706f0 Call Trace: <TASK> ? __die+0x23/0x70 ? page_fault_oops+0x171/0x4e0 ?

		exc_page_fault+0x7f/0x180 ? asm_exc_page_fault+0x26/0x30 ? vmw_du_cursor_plane_cleanup_fb+0x124/0x140 [vmwgfx] drm_atomic_helper_cleanup_planes+0x9b/0xc0 commit_tail+0xd1/0x130 drm_atomic_helper_commit+0x11a/0x140 drm_atomic_commit+0x97/0xd0 ? __pfx___drm_printfn_info+0x10/0x10 drm_atomic_helper_update_plane+0xf5/0x160 drm_mode_cursor_universal+0x10e/0x270 drm_mode_cursor_common+0x102/0x230 ? __pfx_drm_mode_cursor2_ioctl+0x10/0x10 drm_ioctl_kernel+0xb2/0x110 drm_ioctl+0x26d/0x4b0 ? __pfx_drm_mode_cursor2_ioctl+0x10/0x10 ? __pfx_drm_ioctl+0x10/0x10 vmw_generic_ioctl+0xa4/0x110 [vmwgfx] __x64_sys_ioctl+0x94/0xd0 do_syscall_64+0x61/0xe0 ? __x64_sys_ioctl+0xaf/0xd0 ? syscall_exit_to_user_mode+0x2b/0x40 ? do_syscall_64+0x70/0xe0 ? __x64_sys_ioctl+0xaf/0xd0 ? syscall_exit_to_user_mode+0x2b/0x40 ? do_syscall_64+0x70/0xe0 ? exc_page_fault+0x7f/0x180 entry_SYSCALL_64_after_hwframe+0x6e/0x76 RIP: 0033:0x7f1e93f279ed Code: 04 25 28 00 00 00 48 89 45 c8 31 c0 48 8d 45 10 c7 45 b0 10 00 00 00 48 89 45 b8 48 8d 45 d0 48 89 45 c0 b8 10 00 00 00 0f 05 <89> c2 3d 00 f0 ff f> RSP: 002b:00007ffca0faf600 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 000055db876ed2c0 RCX: 00007f1e93f279ed RDX: 00007ffca0faf6c0 RSI: 00000000c02464bb RDI: 0000000000000015 RBP: 00007ffca0faf650 R08: 000055db87184010 R09: 0000000000000007 R10: 000055db886471a0 R11: 0000000000000246 R12: 00007ffca0faf6c0 R13: 00000000c02464bb R14: 0000000000000015 R15: 00007ffca0faf790 </TASK> Modules linked in: snd_seq_dummy snd_hrtimer nf_conntrack_netbios_ns nf_conntrack_broadcast

		nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib nft_reject_ine> CR2: 0000000000000028 ---[end trace 0000000000000000]--- RIP: 0010:vmw_du_cursor_plane_cleanup_fb+0x124/0x140 [vmwgfx] Code: 00 00 00 75 3a 48 83 c4 10 5b 5d c3 cc cc cc cc 48 8b b3 a8 00 00 00 48 c7 c7 99 90 43 c0 e8 93 c5 db ca 48 8b 83 a8 00 00 00 <48> 8b 78 28 e8 e3 f> RSP: 0018:ffffb6b98216fa80 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffff969d84cdcb00 RCX: 0000000000000027 RDX: 0000000000000000 RSI: 0000000000000001 RDI: ffff969e75f21600 RBP: ffff969d4143 ---truncated---
CVE-2023-52653	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: fix a memleak in gss_import_v2_context The ctx->mech_used.data allocated by kmemdup is not freed in neither gss_import_v2_context nor it only caller gss_krb5_import_sec_context, which frees ctx on error. Thus, this patch reform the last call of gss_import_v2_context to the gss_krb5_import_ctx_v2, preventing the memleak while keepping the return formation.
CVE-2023-52658	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: Revert "net/mlx5: Block entering switchdev mode with ns inconsistency" This reverts commit 662404b24a4c4d839839ed25e3097571f5938b9b. The revert is required due to the suspicion it is not good for anything and cause crash.
CVE-2023-52	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: fix a memleak in vmw_gmrid_man_get_node When ida_alloc_max fails, resources allocated before should be freed, including *res allocated by kmalloc and ttm_resource_init.

662		
CVE-2023-52679	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: of: Fix double free in of_parse_phandle_with_args_map In of_parse_phandle_with_args_map() the inner loop that iterates through the map entries calls of_node_put(new) to free the reference acquired by the previous iteration of the inner loop. This assumes that the value of "new" is NULL on the first iteration of the inner loop. Make sure that this is true in all iterations of the outer loop by setting "new" to NULL after its value is assigned to "cur". Extend the unittest to detect the double free and add an additional test case that actually triggers this path.
CVE-2023-52707	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: sched/psi: Fix use-after-free in ep_remove_wait_queue() If a non-root cgroup gets removed when there is a thread that registered trigger and is polling on a pressure file within the cgroup, the polling waitqueue gets freed in the following path: do_rmdir cgroup_rmdir kernfs_drain_open_files cgroup_file_release cgroup_pressure_release psi_trigger_destroy However, the polling thread still has a reference to the pressure file and will access the freed waitqueue when the file is closed or upon exit: fput ep_eventpoll_release ep_free ep_remove_wait_queue remove_wait_queue This results in use-after-free as pasted below. The fundamental problem here is that cgroup_file_release() (and consequently waitqueue's lifetime) is not tied to the file's real lifetime. Using wake_up_pollfree() here might be less than ideal, but it is in line with the comment at commit 42288cb44c4b ("wait: add wake_up_pollfree()") since the waitqueue's lifetime is not tied to file's one and can be considered as another special case. While this would be fixable by somehow

		making cgroup_file_release() be tied to the fput(), it would require sizable refactoring at cgroups or higher layer which might be more justifiable if we identify more cases like this. BUG: KASAN: use-after-free in _raw_spin_lock_irqsave+0x60/0xc0 Write of size 4 at addr ffff88810e625328 by task a.out/4404 CPU: 19 PID: 4404 Comm: a.out Not tainted 6.2.0-rc6 #38 Hardware name: Amazon EC2 c5a.8xlarge/, BIOS 1.0 10/16/2017 Call Trace: <TASK> dump_stack_lvl+0x73/0xa0 print_report+0x16c/0x4e0 kasan_report+0xc3/0xf0 kasan_check_range+0x2d2/0x310 _raw_spin_lock_irqsave+0x60/0xc0 remove_wait_queue+0x1a/0xa0 ep_free+0x12c/0x170 ep_eventpoll_release+0x26/0x30 __fput+0x202/0x400 task_work_run+0x11d/0x170 do_exit+0x495/0x1130 do_group_exit+0x100/0x100 get_signal+0xd67/0xde0 arch_do_signal_or_restart+0x2a/0x2b0 exit_to_user_mode_prepare+0x94/0x100 syscall_exit_to_user_mode+0x20/0x40 do_syscall_64+0x52/0x90 entry_SYSCALL_64_after_hwframe+0x63/0xcd </TASK> Allocated by task 4404: kasan_set_track+0x3d/0x60 __kasan_kmalloc+0x85/0x90 psi_trigger_create+0x113/0x3e0 pressure_write+0x146/0x2e0 cgroup_file_write+0x11c/0x250 kernfs_fop_write_iter+0x186/0x220 vfs_write+0x3d8/0x5c0 ksys_write+0x90/0x110 do_syscall_64+0x43/0x90 entry_SYSCALL_64_after_hwframe+0x63/0xcd Freed by task 4407: kasan_set_track+0x3d/0x60 kasan_save_free_info+0x27/0x40 ____kasan_slab_free+0x11d/0x170 slab_free_freelist_hook+0x87/0x150 __kmem_cache_free+0xcb/0x180 psi_trigger_destroy+0x2e8/0x310 cgroup_file_release+0x4f/0xb0

		kernfs_drain_open_files+0x165/0x1f0 kernfs_drain+0x162/0x1a0 __kernfs_remove+0x1fb/0x310 kernfs_remove_by_name_ns+0x95/0xe0 cgroup_addrm_files+0x67f/0x700 cgroup_destroy_locked+0x283/0x3c0 cgroup_rmdir+0x29/0x100 kernfs_iop_rmdir+0xd1/0x140 vfs_rmdir+0xfe/0x240 do_rmdir+0x13d/0x280 __x64_sys_rmdir+0x2c/0x30 do_syscall_64+0x43/0x90 entry_SYSCALL_64_after_hwframe+0x63/0xcd
CVE-2023-52730	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: mmc: sdio: fix possible resource leaks in some error paths If sdio_add_func() or sdio_init_func() fails, sdio_remove_func() can not release the resources, because the sdio function is not presented in these two cases, it won't call of_node_put() or put_device(). To fix these leaks, make sdio_func_present() only control whether device_del() needs to be called or not, then always call of_node_put() and put_device(). In error case in sdio_init_func(), the reference of 'card->dev' is not get, to avoid redundant put in sdio_free_func_cis(), move the get_device() to sdio_alloc_func() and put_device() to sdio_release_func(), it can keep the get/put function be balanced. Without this patch, while doing fault inject test, it can get the following leak reports, after this fix, the leak is gone. unreferenced object 0xffff888112514000 (size 2048): comm "kworker/3:2", pid 65, jiffies 4294741614 (age 124.774s) hex dump (first 32 bytes): 00 e0 6f 12 81 88 ff ff 60 58 8d 06 81 88 ff ff ..o.....`X..... 10 40 51 12 81 88 ff ff 10 40 51 12 81 88 ff ff .@Q.....@Q..... backtrace: [<000000009e5931da>] kmalloc_trace+0x21/0x110 [<000000002f839ccb>] mmc_alloc_card+0x38/0xb0 [mmc_core] [<0000000004adcbf6>] mmc_sdio_init_card+0xde/0x170 [mmc_core] [<000000007538fea0>] mmc_attach_sdio+0xcb/0x1b0 [mmc_core] [<00000000d4fdeba7>] mmc_rescan+0x54a/0x640 [mmc_core] unreferenced

		object 0xffff888112511000 (size 2048): comm "kworker/3:2", pid 65, jiffies 4294741623 (age 124.766s) hex dump (first 32 bytes): 00 40 51 12 81 88 ff ff e0 58 8d 06 81 88 ff ff .@Q.....X..... 10 10 51 12 81 88 ff ff 10 10 51 12 81 88 ff ff ..Q.....Q..... backtrace: [<000000009e5931da>] kmalloc_trace+0x21/0x110 [<00000000fcbe706c>] sdio_alloc_func+0x35/0x100 [mmc_core] [<00000000c68f4b50>] mmc_attach_sdio.cold.18+0xb1/0x395 [mmc_core] [<00000000d4fdeba7>] mmc_rescan+0x54a/0x640 [mmc_core]
CVE-2023-52756		Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2023-52762	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: virtio-blk: fix implicit overflow on virtio_max_dma_size The following codes have an implicit conversion from size_t to u32: (u32)max_size = (size_t)virtio_max_dma_size(vdev); This may lead overflow, Ex (size_t)4G -> (u32)0. Once virtio_max_dma_size() has a larger size than U32_MAX, use U32_MAX instead.
CVE-2023-52764	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: media: gspca: cpia1: shift-out-of-bounds in set_flicker Syzkaller reported the following issue: UBSAN: shift-out-of-bounds in drivers/media/usb/gspca/cpia1.c:1031:27 shift exponent 245 is too large for 32-bit type 'int' When the value of the variable "sd->params.exposure.gain" exceeds the number of bits in an integer, a shift-out-of-bounds error is

		reported. It is triggered because the variable "currentexp" cannot be left-shifted by more than the number of bits in an integer. In order to avoid invalid range during left-shift, the conditional expression is added.
CVE-2023-52775	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: net/smc: avoid data corruption caused by decline We found a data corruption issue during testing of SMC-R on Redis applications. The benchmark has a low probability of reporting a strange error as shown below. "Error: Protocol error, got "\xe2" as reply type byte" Finally, we found that the retrieved error data was as follows: 0xE2 0xD4 0xC3 0xD9 0x04 0x00 0x2C 0x20 0xA6 0x56 0x00 0x16 0x3E 0x0C 0xCB 0x04 0x02 0x01 0x00 0x00 0x20 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0xE2 It is quite obvious that this is a SMC DECLINE message, which means that the applications received SMC protocol message. We found that this was caused by the following situations: client server ¦ clc proposal ----------> ¦ clc accept <---------- ¦ clc confirm ----------> wait llc confirm send llc confirm ¦failed llc confirm ¦ x------ (after 2s)timeout wait llc confirm rsp wait decline (after 1s) timeout (after 2s) timeout ¦ decline ----------> ¦ decline <---------- As a result, a decline message was sent in the implementation, and this message was read from TCP by the already-fallback connection. This patch double the client timeout as 2x of the server value, With this simple change, the Decline messages should never cross or collide (during Confirm link timeout). This issue requires an immediate solution, since the protocol updates involve a more long-term solution.
CVE-2023-	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: fix gtk offload status event locking The ath11k active pdevs are protected by RCU but the gtk offload status event handling code calling

52 77 7		ath11k_mac_get_arvif_by_vdev_id() was not marked as a read-side critical section. Mark the code in question as an RCU read-side critical section to avoid any potential use-after-free issues. Compile tested only.
CVE-2023-52784	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: bonding: stop the device in bond_setup_by_slave() Commit 9eed321cde22 ("net: lapbether: only support ethernet devices") has been able to keep syzbot away from net/lapb, until today. In the following splat [1], the issue is that a lapbether device has been created on a bonding device without members. Then adding a non ARPHRD_ETHER member forced the bonding master to change its type. The fix is to make sure we call dev_close() in bond_setup_by_slave() so that the potential linked lapbether devices (or any other devices having assumptions on the physical device) are removed. A similar bug has been addressed in commit 40baec225765 ("bonding: fix panic on non-ARPHRD_ETHER enslave failure") [1] skbuff: skb_under_panic: text:ffff800089508810 len:44 put:40 head:ffff0000c78e7c00 data:ffff0000c78e7bea tail:0x16 end:0x140 dev:bond0 kernel BUG at net/core/skbuff.c:192 ! Internal error: Oops - BUG: 00000000f2000800 [#1] PREEMPT SMP Modules linked in: CPU: 0 PID: 6007 Comm: syz-executor383 Not tainted 6.6.0-rc3-syzkaller-gbf6547d8715b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/04/2023 pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : skb_panic net/core/skbuff.c:188 [inline] pc : skb_under_panic+0x13c/0x140 net/core/skbuff.c:202 lr : skb_panic net/core/skbuff.c:188 [inline] lr : skb_under_panic+0x13c/0x140 net/core/skbuff.c:202 sp : ffff800096a06aa0 x29: ffff800096a06ab0 x28: ffff800096a06ba0 x27: dfff800000000000 x26: ffff0000ce9b9b50 x25: 0000000000000016 x24: ffff0000c78e7bea x23:

		ffff0000c78e7c00 x22: 000000000000002c x21: 0000000000000140 x20: 0000000000000028 x19: ffff800089508810 x18: ffff800096a06100 x17: 0000000000000000 x16: ffff80008a629a3c x15: 0000000000000001 x14: 1fffe00036837a32 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000201 x10: 0000000000000000 x9 : cb50b496c519aa00 x8 : cb50b496c519aa00 x7 : 0000000000000001 x6 : 0000000000000001 x5 : ffff800096a063b8 x4 : ffff80008e280f80 x3 : ffff8000805ad11c x2 : 0000000000000001 x1 : 0000000100000201 x0 : 0000000000000086 Call trace: skb_panic net/core/skbuff.c:188 [inline] skb_under_panic+0x13c/0x140 net/core/skbuff.c:202 skb_push+0xf0/0x108 net/core/skbuff.c:2446 ip6gre_header+0xbc/0x738 net/ipv6/ip6_gre.c:1384 dev_hard_header include/linux/netdevice.h:3136 [inline] lapbeth_data_transmit+0x1c4/0x298 drivers/net/wan/lapbether.c:257 lapb_data_transmit+0x8c/0xb0 net/lapb/lapb_iface.c:447 lapb_transmit_buffer+0x178/0x204 net/lapb/lapb_out.c:149 lapb_send_control+0x220/0x320 net/lapb/lapb_subr.c:251 __lapb_disconnect_request+0x9c/0x17c net/lapb/lapb_iface.c:326 lapb_device_event+0x288/0x4e0 net/lapb/lapb_iface.c:492 notifier_call_chain+0x1a4/0x510 kernel/notifier.c:93 raw_notifier_call_chain+0x3c/0x50 kernel/notifier.c:461 call_netdevice_notifiers_info net/core/dev.c:1970 [inline] call_netdevice_notifiers_extack net/core/dev.c:2008 [inline] call_netdevice_notifiers net/core/dev.c:2022 [inline] __dev_close_many+0x1b8/0x3c4 net/core/dev.c:1508 dev_close_many+0x1e0/0x470 net/core/dev.c:1559 dev_close+0x174/0x250 net/core/dev.c:1585 lapbeth_device_event+0x2e4/0x958 drivers/net/wan/lapbether.c:466

		notifier_call_chain+0x1a4/0x510 kernel/notifier.c:93 raw_notifier_call_chain+0x3c/0x50 kernel/notifier.c:461 call_netdevice_notifiers_info net/core/dev.c:1970 [inline] call_netdevice_notifiers_extack net/core/dev.c:2008 [inline] call_netdevice_notifiers net/core/dev.c:2022 [inline] __dev_close_many+0x1b8/0x3c4 net/core/dev.c:1508 dev_close_many+0x1e0/0x470 net/core/dev.c:1559 dev_close+0x174/0x250 net/core/dev.c:1585 bond_enslave+0x2298/0x30cc drivers/net/bonding/bond_main.c:2332 bond_do_ioctl+0x268/0xc64 drivers/net/bonding/bond_main.c:4539 dev_ifsioc+0x754/0x9ac dev_ioctl+0x4d8/0xd34 net/core/dev_ioctl.c:786 sock_do_ioctl+0x1d4/0x2d0 net/socket.c:1217 sock_ioctl+0x4e8/0x834 net/socket.c:1322 vfs_ioctl fs/ioctl.c:51 [inline] __do_ --- truncated---
CVE-2023-52791	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: i2c: core: Run atomic i2c xfer when !preemptible Since bae1d3a05a8b, i2c transfers are non-atomic if preemption is disabled. However, non-atomic i2c transfers require preemption (e.g. in wait_for_completion() while waiting for the DMA). panic() calls preempt_disable_notrace() before calling emergency_restart(). Therefore, if an i2c device is used for the restart, the xfer should be atomic. This avoids warnings like: [12.667612] WARNING: CPU: 1 PID: 1 at kernel/rcu/tree_plugin.h:318 rcu_note_context_switch+0x33c/0x6b0 [12.676926] Voluntary context switch within RCU read-side critical section! ... [12.742376] schedule_timeout from wait_for_completion_timeout+0x90/0x114 [12.749179] wait_for_completion_timeout from tegra_i2c_wait_completion+0x40/0x70 ... [12.994527] atomic_notifier_call_chain from machine_restart+0x34/0x58 [13.001050] machine_restart

		from panic+0x2a8/0x32c Use !preemptible() instead, which is basically the same check as pre-v5.2.
CVE-2023-52796	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: ipvlan: add ipvlan_route_v6_outbound() helper Inspired by syzbot reports using a stack of multiple ipvlan devices. Reduce stack size needed in ipvlan_process_v6_outbound() by moving the flowi6 struct used for the route lookup in an non inlined helper. ipvlan_route_v6_outbound() needs 120 bytes on the stack, immediately reclaimed. Also make sure ipvlan_process_v4_outbound() is not inlined. We might also have to lower MAX_NEST_DEV, because only syzbot uses setups with more than four stacked devices. BUG: TASK stack guard page was hit at ffffc9000e803ff8 (stack is ffffc9000e804000..ffffc9000e808000) stack guard page: 0000 [#1] SMP KASAN CPU: 0 PID: 13442 Comm: syz-executor.4 Not tainted 6.1.52-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/09/2023 RIP: 0010:kasan_check_range+0x4/0x2a0 mm/kasan/generic.c:188 Code: 48 01 c6 48 89 c7 e8 db 4e c1 03 31 c0 5d c3 cc 0f 0b eb 02 0f 0b b8 ea ff ff ff 5d c3 cc 00 00 cc cc 00 00 cc cc 55 48 89 e5 <41> 57 41 56 41 55 41 54 53 b0 01 48 85 f6 0f 84 a4 01 00 00 48 89 RSP: 0018:ffffc9000e804000 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: ffffffff817e5bf2 RDX: 0000000000000000 RSI: 0000000000000008 RDI: ffffffff887c6568 RBP: ffffc9000e804000 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: dffffc0000000001 R12: 1ffff92001d0080c R13: dffffc0000000000 R14: ffffffff87e6b100 R15: 0000000000000000 FS: 00007fd0c55826c0(0000) GS:ffff8881f6800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffc9000e803ff8 CR3: 0000000170ef7000 CR4:

		00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <#DF> </#DF> <TASK> [<ffffffff81f281d1>] __kasan_check_read+0x11/0x20 mm/kasan/shadow.c:31 [<ffffffff817e5bf2>] instrument_atomic_read include/linux/instrumented.h:72 [inline] [<ffffffff817e5bf2>] _test_bit include/asm-generic/bitops/instrumented-non-atomic.h:141 [inline] [<ffffffff817e5bf2>] cpumask_test_cpu include/linux/cpumask.h:506 [inline] [<ffffffff817e5bf2>] cpu_online include/linux/cpumask.h:1092 [inline] [<ffffffff817e5bf2>] trace_lock_acquire include/trace/events/lock.h:24 [inline] [<ffffffff817e5bf2>] lock_acquire+0xe2/0x590 kernel/locking/lockdep.c:5632 [<ffffffff8563221e>] rcu_lock_acquire+0x2e/0x40 include/linux/rcupdate.h:306 [<ffffffff8561464d>] rcu_read_lock include/linux/rcupdate.h:747 [inline] [<ffffffff8561464d>] ip6_pol_route+0x15d/0x1440 net/ipv6/route.c:2221 [<ffffffff85618120>] ip6_pol_route_output+0x50/0x80 net/ipv6/route.c:2606 [<ffffffff856f65b5>] pol_lookup_func include/net/ip6_fib.h:584 [inline] [<ffffffff856f65b5>] fib6_rule_lookup+0x265/0x620 net/ipv6/fib6_rules.c:116 [<ffffffff85618009>] ip6_route_output_flags_noref+0x2d9/0x3a0 net/ipv6/route.c:2638 [<ffffffff8561821a>] ip6_route_output_flags+0xca/0x340 net/ipv6/route.c:2651 [<ffffffff838bd5a3>] ip6_route_output include/net/ip6_route.h:100 [inline] [<ffffffff838bd5a3>] ipvlan_process_v6_outbound drivers/net/ipvlan/ipvlan_core.c:473 [inline] [<ffffffff838bd5a3>] ipvlan_process_outbound drivers/net/ipvlan/ipvlan_core.c:529 [inline] [<ffffffff838bd5a3>] ipvlan_xmit_mode_l3 drivers/net/ipvlan/ipvlan_core.c:602 [inline] [<ffffffff838bd5a3>] ipvlan_queue_xmit+0xc33/0x1be0

		drivers/net/ipvlan/ipvlan_core.c:677 [<ffffffff838c2909>] ipvlan_start_xmit+0x49/0x100 drivers/net/ipvlan/ipvlan_main.c:229 [<ffffffff84d03900>] netdev_start_xmit include/linux/netdevice.h:4966 [inline] [<ffffffff84d03900>] xmit_one net/core/dev.c:3644 [inline] [<ffffffff84d03900>] dev_hard_start_xmit+0x320/0x980 net/core/dev.c:3660 [<ffffffff84d080e2>] __dev_queue_xmit+0x16b2/0x3370 net/core/dev.c:4324 [<ffffffff855ce4cd>] dev_queue_xmit include/linux/netdevice.h:3067 [inline] [<ffffffff855ce4cd>] neigh_hh_output include/net/neighbour.h:529 [inline] [<f ---truncated---
CVE-2023-52803	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: Fix RPC client cleaned up the freed pipefs dentries RPC client pipefs dentries cleanup is in separated rpc_remove_pipedir() workqueue,which takes care about pipefs superblock locking. In some special scenarios, when kernel frees the pipefs sb of the current client and immediately alloctes a new pipefs sb, rpc_remove_pipedir function would misjudge the existence of pipefs sb which is not the one it used to hold. As a result, the rpc_remove_pipedir would clean the released freed pipefs dentries. To fix this issue, rpc_remove_pipedir should check whether the current pipefs sb is consistent with the original pipefs sb. This error can be catched by KASAN: ========== [250.497700] BUG: KASAN: slab-use-after-free in dget_parent+0x195/0x200 [250.498315] Read of size 4 at addr ffff88800a2ab804 by task kworker/0:18/106503 [250.500549] Workqueue: events rpc_free_client_work [250.501001] Call Trace: [250.502880] kasan_report+0xb6/0xf0 [250.503209] ? dget_parent+0x195/0x200 [250.503561] dget_parent+0x195/0x200 [250.503897] ? __pfx_rpc_clntdir_depopulate+0x10/0x10 [250.504384]

		rpc_rmdir_depopulate+0x1b/0x90 [250.504781] rpc_remove_client_dir+0xf5/0x150 [250.505195] rpc_free_client_work+0xe4/0x230 [250.505598] process_one_work+0x8ee/0x13b0 ... [22.039056] Allocated by task 244: [22.039390] kasan_save_stack+0x22/0x50 [22.039758] kasan_set_track+0x25/0x30 [22.040109] __kasan_slab_alloc+0x59/0x70 [22.040487] kmem_cache_alloc_lru+0xf0/0x240 [22.040889] __d_alloc+0x31/0x8e0 [22.041207] d_alloc+0x44/0x1f0 [22.041514] __rpc_lookup_create_exclusive+0x11c/0x140 [22.041987] rpc_mkdir_populate.constprop.0+0x5f/0x110 [22.042459] rpc_create_client_dir+0x34/0x150 [22.042874] rpc_setup_pipedir_sb+0x102/0x1c0 [22.043284] rpc_client_register+0x136/0x4e0 [22.043689] rpc_new_client+0x911/0x1020 [22.044057] rpc_create_xprt+0xcb/0x370 [22.044417] rpc_create+0x36b/0x6c0 ... [22.049524] Freed by task 0: [22.049803] kasan_save_stack+0x22/0x50 [22.050165] kasan_set_track+0x25/0x30 [22.050520] kasan_save_free_info+0x2b/0x50 [22.050921] __kasan_slab_free+0x10e/0x1a0 [22.051306] kmem_cache_free+0xa5/0x390 [22.051667] rcu_core+0x62c/0x1930 [22.051995] __do_softirq+0x165/0x52a [22.052347] [22.052503] Last potentially related work creation: [22.052952] kasan_save_stack+0x22/0x50 [22.053313] __kasan_record_aux_stack+0x8e/0xa0 [22.053739] __call_rcu_common.constprop.0+0x6b/0x8b0 [22.054209] dentry_free+0xb2/0x140 [22.054540] __dentry_kill+0x3be/0x540 [22.054900] shrink_dentry_list+0x199/0x510 [22.055293] shrink_dcache_parent+0x190/0x240 [22.055703] do_one_tree+0x11/0x40 [22.056028] shrink_dcache_for_umount+0x61/0x140 [22.056461] generic_shutdown_super+0x70/0x590 [22.056879]

		kill_anon_super+0x3a/0x60 [22.057234] rpc_kill_sb+0x121/0x200
CVE-2023-52811	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: scsi: ibmvfc: Remove BUG_ON in the case of an empty event pool In practice the driver should never send more commands than are allocated to a queue's event pool. In the unlikely event that this happens, the code asserts a BUG_ON, and in the case that the kernel is not configured to crash on panic returns a junk event pointer from the empty event list causing things to spiral from there. This BUG_ON is a historical artifact of the ibmvfc driver first being upstreamed, and it is well known now that the use of BUG_ON is bad practice except in the most unrecoverable scenario. There is nothing about this scenario that prevents the driver from recovering and carrying on. Remove the BUG_ON in question from ibmvfc_get_event() and return a NULL pointer in the case of an empty event pool. Update all call sites to ibmvfc_get_event() to check for a NULL pointer and perfrom the appropriate failure or recovery action.
CVE-2023-52832	9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: don't return unset power in ieee80211_get_tx_power() We can get a UBSAN warning if ieee80211_get_tx_power() returns the INT_MIN value mac80211 internally uses for "unset power level". UBSAN: signed-integer-overflow in net/wireless/nl80211.c:3816:5 -2147483648 * 100 cannot be represented in type 'int' CPU: 0 PID: 20433 Comm: insmod Tainted: G WC OE Call Trace: dump_stack+0x74/0x92 ubsan_epilogue+0x9/0x50 handle_overflow+0x8d/0xd0 __ubsan_handle_mul_overflow+0xe/0x10 nl80211_send_iface+0x688/0x6b0 [cfg80211] [...] cfg80211_register_wdev+0x78/0xb0 [cfg80211] cfg80211_netdev_notifier_call+0x200/0x620 [cfg80211] [...] ieee80211_if_add+0x60e/0x8f0 [mac80211]

		ieee80211_register_hw+0xda5/0x1170 [mac80211] In this case, simply return an error instead, to indicate that no data is available.
CVE-2023-52834	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: atl1c: Work around the DMA RX overflow issue This is based on alx driver commit 881d0327db37 ("net: alx: Work around the DMA RX overflow issue"). The alx and atl1c drivers had RX overflow error which was why a custom allocator was created to avoid certain addresses. The simpler workaround then created for alx driver, but not for atl1c due to lack of tester. Instead of using a custom allocator, check the allocated skb address and use skb_reserve() to move away from problematic 0x...fc0 address. Tested on AR8131 on Acer 4540.
CVE-2023-52845	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: tipc: Change nla_policy for bearer-related names to NLA_NUL_STRING syzbot reported the following uninit-value access issue [1]: ========== ====== BUG: KMSAN: uninit-value in strlen lib/string.c:418 [inline] BUG: KMSAN: uninit-value in strstr+0xb8/0x2f0 lib/string.c:756 strlen lib/string.c:418 [inline] strstr+0xb8/0x2f0 lib/string.c:756 tipc_nl_node_reset_link_stats+0x3ea/0xb50 net/tipc/node.c:2595 genl_family_rcv_msg_doit net/netlink/genetlink.c:971 [inline] genl_family_rcv_msg net/netlink/genetlink.c:1051 [inline] genl_rcv_msg+0x11ec/0x1290 net/netlink/genetlink.c:1066 netlink_rcv_skb+0x371/0x650 net/netlink/af_netlink.c:2545 genl_rcv+0x40/0x60 net/netlink/genetlink.c:1075 netlink_unicast_kernel net/netlink/af_netlink.c:1342 [inline] netlink_unicast+0xf47/0x1250 net/netlink/af_netlink.c:1368

		netlink_sendmsg+0x1238/0x13d0 net/netlink/af_netlink.c:1910 sock_sendmsg_nosec net/socket.c:730 [inline] sock_sendmsg net/socket.c:753 [inline] ____sys_sendmsg+0x9c2/0xd60 net/socket.c:2541 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2595 __sys_sendmsg net/socket.c:2624 [inline] __do_sys_sendmsg net/socket.c:2633 [inline] __se_sys_sendmsg net/socket.c:2631 [inline] __x64_sys_sendmsg+0x307/0x490 net/socket.c:2631 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x41/0xc0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd Uninit was created at: slab_post_alloc_hook+0x12f/0xb70 mm/slab.h:767 slab_alloc_node mm/slub.c:3478 [inline] kmem_cache_alloc_node+0x577/0xa80 mm/slub.c:3523 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:559 __alloc_skb+0x318/0x740 net/core/skbuff.c:650 alloc_skb include/linux/skbuff.h:1286 [inline] netlink_alloc_large_skb net/netlink/af_netlink.c:1214 [inline] netlink_sendmsg+0xb34/0x13d0 net/netlink/af_netlink.c:1885 sock_sendmsg_nosec net/socket.c:730 [inline] sock_sendmsg net/socket.c:753 [inline] ____sys_sendmsg+0x9c2/0xd60 net/socket.c:2541 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2595 __sys_sendmsg net/socket.c:2624 [inline] __do_sys_sendmsg net/socket.c:2633 [inline] __se_sys_sendmsg net/socket.c:2631 [inline] __x64_sys_sendmsg+0x307/0x490 net/socket.c:2631 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x41/0xc0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x63/0xcd TIPC bearer-related names including link names must be null-terminated strings. If a link name which is not null-terminated is passed through netlink, strstr() and similar functions can cause buffer overrun. This causes the above issue. This patch changes the nla_policy for bearer-related names from NLA_STRING to NLA_NUL_STRING. This

		resolves the issue by ensuring that only null-terminated strings are accepted as bearer-related names. syzbot reported similar uninit-value issue related to bearer names [2]. The root cause of this issue is that a non-null-terminated bearer name was passed. This patch also resolved this issue.
CVE-2023-5678	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)	Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS

		implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.
CVE-2024-0727	5.5 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H)	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.
CVE-2024-11187	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	It is possible to construct a zone such that some queries to it will generate responses containing numerous records in the Additional section. An attacker sending many such queries can cause either the authoritative server itself or an independent resolver to use disproportionate resources processing the queries. Zones will usually need to have been deliberately crafted to attack this exposure. This issue affects BIND 9 versions 9.11.0 through 9.11.37, 9.16.0 through 9.16.50, 9.18.0 through 9.18.32, 9.20.0 through 9.20.4, 9.21.0 through 9.21.3, 9.11.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.50-S1, and 9.18.11-S1 through 9.18.32-S1.

CVE-2024-12085	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	A flaw was found in rsync which could be triggered when rsync compares file checksums. This flaw allows an attacker to manipulate the checksum length (s2length) to cause a comparison between a checksum and uninitialized memory and leak one byte of uninitialized stack data at a time.
CVE-2024-1317 6	4.1 (CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L)	Issue summary: A timing side-channel which could potentially allow recovering the private key exists in the ECDSA signature computation. Impact summary: A timing side-channel in ECDSA signature computations could allow recovering the private key by an attacker. However, measuring the timing would require either local access to the signing application or a very fast network connection with low latency. There is a timing signal of around 300 nanoseconds when the top word of the inverted ECDSA nonce value is zero. This can happen with significant probability only for some of the supported elliptic curves. In particular the NIST P-521 curve is affected. To be able to measure this leak, the attacker process must either be located in the same physical computer or must have a very fast network connection with low latency. For that reason the severity of this vulnerability is Low. The FIPS modules in 3.4, 3.3, 3.2, 3.1 and 3.0 are affected by this issue.
CVE-2024-1737	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	Resolver caches and authoritative zone databases that hold significant numbers of RRs for the same hostname (of any RTYPE) can suffer from degraded performance as content is being added or updated, and also when handling client queries for this name. This issue affects BIND 9 versions 9.11.0 through 9.11.37, 9.16.0 through 9.16.50, 9.18.0 through 9.18.27, 9.19.0 through 9.19.24, 9.11.4-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.50-S1, and 9.18.11-S1 through 9.18.27-S1.

CVE-2024-19775	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	If a server hosts a zone containing a "KEY" Resource Record, or a resolver DNSSEC-validates a "KEY" Resource Record from a DNSSEC-signed domain in cache, a client can exhaust resolver CPU resources by sending a stream of SIG(0) signed requests. This issue affects BIND 9 versions 9.0.0 through 9.11.37, 9.16.0 through 9.16.50, 9.18.0 through 9.18.27, 9.19.0 through 9.19.24, 9.9.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.49-S1, and 9.18.11-S1 through 9.18.27-S1.
CVE-2024-20918	7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).

CVE-2024-20919	5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2024-20921	5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs.

		This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2024-20926	5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21; Oracle GraalVM for JDK: 17.0.9; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2024-20	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9,

945		21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition executes to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 4.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).
CVE-2024-20952	7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Security). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to

		Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).
CVE-2024-21011	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u401, 8u401-perf, 11.0.22, 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).

CVE-2024-21012	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 11.0.22, 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2024-21068	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u401-perf, 11.0.22, 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2 and 22; Oracle GraalVM Enterprise Edition: 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition

		accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2024-21085	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Oracle Java SE: 8u401, 8u401-perf, 11.0.22; Oracle GraalVM Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2024-	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u401, 8u401-perf,

21 09 4		11.0.22, 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CV E- 20 24- 21 13 1	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java

		deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2024-21138	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2024-21	4.8 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition:

140		20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2024-21144	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security.

		This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2024-21145	4.8 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf, 11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2024-	7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u411, 8u411-perf,

21 14 7		11.0.23, 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM for JDK: 17.0.11, 21.0.3, 22.0.1; Oracle GraalVM Enterprise Edition: 20.3.14 and 21.3.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).
CVE-2024-21208	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK,

		Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2024-21210	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)	Vulnerability in Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4 and 23. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2024-21217	3.7 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via

		multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2024-21235	4.8 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java

		applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2024-22019	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	A vulnerability in Node.js HTTP servers allows an attacker to send a specially crafted HTTP request with chunked encoding, leading to resource exhaustion and denial of service (DoS). The server reads an unbounded number of bytes from a single connection, exploiting the lack of limitations on chunk extension bytes. The issue can cause CPU and network bandwidth exhaustion, bypassing standard safeguards like timeouts and body size limits.
CVE-2024-22232	7.7 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)	A specially crafted url can be created which leads to a directory traversal in the salt file server. A malicious user can read an arbitrary file from a Salt master's filesystem.
CVE-2024-24806	7.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)	libuv is a multi-platform support library with a focus on asynchronous I/O. The `uv_getaddrinfo` function in `src/unix/getaddrinfo.c` (and its windows counterpart `src/win/getaddrinfo.c`), truncates hostnames to 256 characters before calling `getaddrinfo`. This behavior can be exploited to create addresses like `0x00007f000001`, which are considered valid by `getaddrinfo` and could allow an attacker to craft payloads that resolve to unintended IP addresses, bypassing developer checks. The vulnerability arises due to how the `hostname_ascii` variable (with a length of 256 bytes) is handled in `uv_getaddrinfo` and subsequently in `uv__idna_toascii`. When the hostname exceeds 256 characters, it gets truncated without a terminating null byte. As a result

		attackers may be able to access internal APIs or for websites (similar to MySpace) that allows users to have `username.example.com` pages. Internal services that crawl or cache these user pages can be exposed to SSRF attacks if a malicious user chooses a long vulnerable username. This issue has been addressed in release version 1.48.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.
CVE-2024-25617	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	Squid is an open source caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to a Collapse of Data into Unsafe Value bug ,Squid may be vulnerable to a Denial of Service attack against HTTP header parsing. This problem allows a remote client or a remote server to perform Denial of Service when sending oversized headers in HTTP messages. In versions of Squid prior to 6.5 this can be achieved if the request_header_max_size or reply_header_max_size settings are unchanged from the default. In Squid version 6.5 and later, the default setting of these parameters is safe. Squid will emit a critical warning in cache.log if the administrator is setting these parameters to unsafe values. Squid will not at this time prevent these settings from being changed to unsafe values. Users are advised to upgrade to version 6.5. There are no known workarounds for this vulnerability. This issue is also tracked as SQUID-2024:2
CVE-2024-2961	7.3 (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H)	The iconv() function in the GNU C Library versions 2.39 and older may overflow the output buffer passed to it by up to 4 bytes when converting strings to the ISO-2022-CN-EXT character set, which may be used to crash an application or overwrite a neighbouring variable.
CVE-20	8.6 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)	less through 653 allows OS command execution via a newline character in the name of a file, because quoting is mishandled in filename.c. Exploitation typically requires

24-32487		use with attacker-controlled file names, such as the files extracted from an untrusted archive. Exploitation also requires the LESSOPEN environment variable, but this is set by default in many common cases.
CVE-2024-33599	8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	nscd: Stack-based buffer overflow in netgroup cache If the Name Service Cache Daemon's (nscd) fixed size cache is exhausted by client requests then a subsequent client request for netgroup data may result in a stack-based buffer overflow. This flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.
CVE-2024-33600	5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)	nscd: Null pointer crashes after notfound response If the Name Service Cache Daemon's (nscd) cache fails to add a not-found netgroup response to the cache, the client request can result in a null pointer dereference. This flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.
CVE-2024-33601	7.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)	nscd: netgroup cache may terminate daemon on memory allocation failure The Name Service Cache Daemon's (nscd) netgroup cache uses xmalloc or xrealloc and these functions may terminate the process due to a memory allocation failure resulting in a denial of service to the clients. The flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.
CVE-2024-33602	7.4 (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	nscd: netgroup cache assumes NSS callback uses in-buffer strings The Name Service Cache Daemon's (nscd) netgroup cache can corrupt memory when the NSS callback does not store all strings in the provided buffer. The flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.

CVE-2024-35893	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_skbmod: prevent kernel-infoleak syzbot found that tcf_skbmod_dump() was copying four bytes from kernel stack to user space [1]. The issue here is that 'struct tc_skbmod' has a four bytes hole. We need to clear the structure before filling fields. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf include/linux/iov_iter.h:29 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance include/linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 instrument_copy_to_user include/linux/instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inline] iterate_and_advance2 include/linux/iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline] _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 copy_to_iter include/linux/uio.h:196 [inline] simple_copy_to_iter net/core/datagram.c:532 [inline] __skb_datagram_iter+0x185/0x1000 net/core/datagram.c:420 skb_copy_datagram_iter+0x5c/0x200 net/core/datagram.c:546 skb_copy_datagram_msg include/linux/skbuff.h:4050 [inline] netlink_recvmsg+0x432/0x1610 net/netlink/af_netlink.c:1962 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x2c4/0x340 net/socket.c:1068 __sys_recvfrom+0x35a/0x5f0 net/socket.c:2242 __do_sys_recvfrom net/socket.c:2260 [inline] __se_sys_recvfrom net/socket.c:2256 [inline] __x64_sys_recvfrom+0x126/0x1d0 net/socket.c:2256

		do_syscall_64+0xd5/0x1f0 entry_SYSCALL_64_after_hwframe+0x6d/0x75 Uninit was stored to memory at: pskb_expand_head+0x30f/0x19d0 net/core/skbuff.c:2253 netlink_trim+0x2c2/0x330 net/netlink/af_netlink.c:1317 netlink_unicast+0x9f/0x1260 net/netlink/af_netlink.c:1351 nlmsg_unicast include/net/netlink.h:1144 [inline] nlmsg_notify+0x21d/0x2f0 net/netlink/af_netlink.c:2610 rtnetlink_send+0x73/0x90 net/core/rtnetlink.c:741 rtnetlink_maybe_send include/linux/rtnetlink.h:17 [inline] tcf_add_notify net/sched/act_api.c:2048 [inline] tcf_action_add net/sched/act_api.c:2071 [inline] tc_ctl_action+0x146e/0x19d0 net/sched/act_api.c:2119 rtnetlink_rcv_msg+0x1737/0x1900 net/core/rtnetlink.c:6595 netlink_rcv_skb+0x375/0x650 net/netlink/af_netlink.c:2559 rtnetlink_rcv+0x34/0x40 net/core/rtnetlink.c:6613 netlink_unicast_kernel net/netlink/af_netlink.c:1335 [inline] netlink_unicast+0xf4c/0x1260 net/netlink/af_netlink.c:1361 netlink_sendmsg+0x10df/0x11f0 net/netlink/af_netlink.c:1905 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ____sys_sendmsg+0x877/0xb60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg+0x307/0x4a0 net/socket.c:2674 do_syscall_64+0xd5/0x1f0 entry_SYSCALL_64_after_hwframe+0x6d/0x75 Uninit was stored to memory at: __nla_put lib/nlattr.c:1041 [inline] nla_put+0x1c6/0x230 lib/nlattr.c:1099 tcf_skbmod_dump+0x23f/0xc20 net/sched/act_skbmod.c:256 tcf_action_dump_old net/sched/act_api.c:1191 [inline]

		tcf_action_dump_1+0x85e/0x970 net/sched/act_api.c:1227 tcf_action_dump+0x1fd/0x460 net/sched/act_api.c:1251 tca_get_fill+0x519/0x7a0 net/sched/act_api.c:1628 tcf_add_notify_msg net/sched/act_api.c:2023 [inline] tcf_add_notify net/sched/act_api.c:2042 [inline] tcf_action_add net/sched/act_api.c:2071 [inline] tc_ctl_action+0x1365/0x19d0 net/sched/act_api.c:2119 rtnetlink_rcv_msg+0x1737/0x1900 net/core/rtnetlink.c:6595 netlink_rcv_skb+0x375/0x650 net/netlink/af_netli ---truncated---
CVE-2024-35896	7.1 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: netfilter: validate user input for expected length I got multiple syzbot reports showing old bugs exposed by BPF after commit 20f2505fb436 ("bpf: Try to avoid kzalloc in cgroup/{s,g}etsockopt") setsockopt() @optlen argument should be taken into account before copying data. BUG: KASAN: slab-out-of-bounds in copy_from_sockptr_offset include/linux/sockptr.h:49 [inline] BUG: KASAN: slab-out-of-bounds in copy_from_sockptr include/linux/sockptr.h:55 [inline] BUG: KASAN: slab-out-of-bounds in do_replace net/ipv4/netfilter/ip_tables.c:1111 [inline] BUG: KASAN: slab-out-of-bounds in do_ipt_set_ctl+0x902/0x3dd0 net/ipv4/netfilter/ip_tables.c:1627 Read of size 96 at addr ffff88802cd73da0 by task syz-executor.4/7238 CPU: 1 PID: 7238 Comm: syz-executor.4 Not tainted 6.9.0-rc2-next-20240403-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:114 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 kasan_check_range+0x282/0x290

		mm/kasan/generic.c:189 __asan_memcpy+0x29/0x70 mm/kasan/shadow.c:105 copy_from_sockptr_offset include/linux/sockptr.h:49 [inline] copy_from_sockptr include/linux/sockptr.h:55 [inline] do_replace net/ipv4/netfilter/ip_tables.c:1111 [inline] do_ipt_set_ctl+0x902/0x3dd0 net/ipv4/netfilter/ip_tables.c:1627 nf_setsockopt+0x295/0x2c0 net/netfilter/nf_sockopt.c:101 do_sock_setsockopt+0x3af/0x720 net/socket.c:2311 __sys_setsockopt+0x1ae/0x250 net/socket.c:2334 __do_sys_setsockopt net/socket.c:2343 [inline] __se_sys_setsockopt net/socket.c:2340 [inline] __x64_sys_setsockopt+0xb5/0xd0 net/socket.c:2340 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x72/0x7a RIP: 0033:0x7fd22067dde9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 e1 20 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007fd21f9ff0c8 EFLAGS: 00000246 ORIG_RAX: 0000000000000036 RAX: ffffffffffffffda RBX: 00007fd2207abf80 RCX: 00007fd22067dde9 RDX: 0000000000000040 RSI: 0000000000000000 RDI: 0000000000000003 RBP: 00007fd2206ca47a R08: 0000000000000001 R09: 0000000000000000 R10: 0000000020000880 R11: 0000000000000246 R12: 0000000000000000 R13: 000000000000000b R14: 00007fd2207abf80 R15: 00007ffd2d0170d8 </TASK> Allocated by task 7238: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:370 [inline] __kasan_kmalloc+0x98/0xb0 mm/kasan/common.c:387 kasan_kmalloc include/linux/kasan.h:211 [inline] __do_kmalloc_node mm/slub.c:4069 [inline] __kmalloc_noprof+0x200/0x410

		mm/slub.c:4082 kmalloc_noprof include/linux/slab.h:664 [inline] __cgroup_bpf_run_filter_setsockopt+0xd47/0x1050 kernel/bpf/cgroup.c:1869 do_sock_setsockopt+0x6b4/0x720 net/socket.c:2293 __sys_setsockopt+0x1ae/0x250 net/socket.c:2334 __do_sys_setsockopt net/socket.c:2343 [inline] __se_sys_setsockopt net/socket.c:2340 [inline] __x64_sys_setsockopt+0xb5/0xd0 net/socket.c:2340 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x72/0x7a The buggy address belongs to the object at ffff88802cd73da0 which belongs to the cache kmalloc-8 of size 8 The buggy address is located 0 bytes inside of allocated 1-byte region [ffff88802cd73da0, ffff88802cd73da1) The buggy address belongs to the physical page: page: refcount:1 mapcount:0 mapping:0000000000000000 index:0xffff88802cd73020 pfn:0x2cd73 flags: 0xfff80000000000(node=0|zone=1|lastcpupid=0xfff) page_type: 0xffffefff(slab) raw: 00fff80000000000 ffff888015041280 dead000000000100 dead000000000122 raw: ffff88802cd73020 000000008080007f 00000001ffffefff 00 ---truncated---
CVE-2024-35897	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: discard table flag update with pending basechain deletion Hook unregistration is deferred to the commit phase, same occurs with hook updates triggered by the table dormant flag. When both commands are combined, this results in deleting a basechain while leaving its hook still registered in the core.
CVE-2024-	6.1 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: flush pending destroy work before exit_net release Similar to 2c9f0293280e ("netfilter: nf_tables: flush pending destroy work before

35 89 9		netlink notifier") to address a race between exit_net and the destroy workqueue. The trace below shows an element to be released via destroy workqueue while exit_net path (triggered via module removal) has already released the set that is used in such transaction. [1360.547789] BUG: KASAN: slab-use-after-free in nf_tables_trans_destroy_work+0x3f5/0x590 [nf_tables] [1360.547861] Read of size 8 at addr ffff888140500cc0 by task kworker/4:1/152465 [1360.547870] CPU: 4 PID: 152465 Comm: kworker/4:1 Not tainted 6.8.0+ #359 [1360.547882] Workqueue: events nf_tables_trans_destroy_work [nf_tables] [1360.547984] Call Trace: [1360.547991] <TASK> [1360.547998] dump_stack_lvl+0x53/0x70 [1360.548014] print_report+0xc4/0x610 [1360.548026] ? __virt_addr_valid+0xba/0x160 [1360.548040] ? __pfx__raw_spin_lock_irqsave+0x10/0x10 [1360.548054] ? nf_tables_trans_destroy_work+0x3f5/0x590 [nf_tables] [1360.548176] kasan_report+0xae/0xe0 [1360.548189] ? nf_tables_trans_destroy_work+0x3f5/0x590 [nf_tables] [1360.548312] nf_tables_trans_destroy_work+0x3f5/0x590 [nf_tables] [1360.548447] ? __pfx_nf_tables_trans_destroy_work+0x10/0x10 [nf_tables] [1360.548577] ? _raw_spin_unlock_irq+0x18/0x30 [1360.548591] process_one_work+0x2f1/0x670 [1360.548610] worker_thread+0x4d3/0x760 [1360.548627] ? __pfx_worker_thread+0x10/0x10 [1360.548640] kthread+0x16b/0x1b0 [1360.548653] ? __pfx_kthread+0x10/0x10 [1360.548665] ret_from_fork+0x2f/0x50 [1360.548679] ? __pfx_kthread+0x10/0x10 [1360.548690] ret_from_fork_asm+0x1a/0x30 [1360.548707] </TASK> [1360.548719] Allocated by task 192061: [1360.548726] kasan_save_stack+0x20/0x40 [1360.548739] kasan_save_track+0x14/0x30 [1360.548750]

		__kasan_kmalloc+0x8f/0xa0 [1360.548760] __kmalloc_node+0x1f1/0x450 [1360.548771] nf_tables_newset+0x10c7/0x1b50 [nf_tables] [1360.548883] nfnetlink_rcv_batch+0xbc4/0xdc0 [nfnetlink] [1360.548909] nfnetlink_rcv+0x1a8/0x1e0 [nfnetlink] [1360.548927] netlink_unicast+0x367/0x4f0 [1360.548935] netlink_sendmsg+0x34b/0x610 [1360.548944] ____sys_sendmsg+0x4d4/0x510 [1360.548953] ___sys_sendmsg+0xc9/0x120 [1360.548961] __sys_sendmsg+0xbe/0x140 [1360.548971] do_syscall_64+0x55/0x120 [1360.548982] entry_SYSCALL_64_after_hwframe+0x55/0x5d [1360.548994] Freed by task 192222: [1360.548999] kasan_save_stack+0x20/0x40 [1360.549009] kasan_save_track+0x14/0x30 [1360.549019] kasan_save_free_info+0x3b/0x60 [1360.549028] poison_slab_object+0x100/0x180 [1360.549036] __kasan_slab_free+0x14/0x30 [1360.549042] kfree+0xb6/0x260 [1360.549049] __nft_release_table+0x473/0x6a0 [nf_tables] [1360.549131] nf_tables_exit_net+0x170/0x240 [nf_tables] [1360.549221] ops_exit_list+0x50/0xa0 [1360.549229] free_exit_list+0x101/0x140 [1360.549236] unregister_pernet_operations+0x107/0x160 [1360.549245] unregister_pernet_subsys+0x1c/0x30 [1360.549254] nf_tables_module_exit+0x43/0x80 [nf_tables] [1360.549345] __do_sys_delete_module+0x253/0x370 [1360.549352] do_syscall_64+0x55/0x120 [1360.549360] entry_SYSCALL_64_after_hwframe+0x55/0x5d (gdb) list *__nft_release_table+0x473 0x1e033 is in __nft_release_table (net/netfilter/nf_tables_api.c:11354). 11349 list_for_each_entry_safe(flowtable, nf, &table->flowtables, list) { 11350 list_del(&flowtable->list); 11351 nft_use_dec(&table->use); 11352 nf_tables_flowtable_destroy(flowtable); 11353 } 11354 list_for_each_entry_safe(set, ns, &table->sets, list) {

		11355 list_del(&set->list); 11356 nft_use_dec(&table->use); 11357 if (set->flags & (NFT_SET_MAP | NFT_SET_OBJECT)) 11358 nft_map_deactivat ---truncated---
CVE-2024-35900	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: reject new basechain after table flag update When dormant flag is toggled, hooks are disabled in the commit phase by iterating over current chains in table (existing and new). The following configuration allows for an inconsistent state: add table x add chain x y { type filter hook input priority 0; } add table x { flags dormant; } add chain x w { type filter hook input priority 1; } which triggers the following warning when trying to unregister chain w which is already unregistered. [127.322252] WARNING: CPU: 7 PID: 1211 at net/netfilter/core.c:50 1 __nf_unregister_net_hook+0x21a/0x260 [...] [127.322519] Call Trace: [127.322521] <TASK> [127.322524] ? __warn+0x9f/0x1a0 [127.322531] ? __nf_unregister_net_hook+0x21a/0x260 [127.322537] ? report_bug+0x1b1/0x1e0 [127.322545] ? handle_bug+0x3c/0x70 [127.322552] ? exc_invalid_op+0x17/0x40 [127.322556] ? asm_exc_invalid_op+0x1a/0x20 [127.322563] ? kasan_save_free_info+0x3b/0x60 [127.322570] ? __nf_unregister_net_hook+0x6a/0x260 [127.322577] ? __nf_unregister_net_hook+0x21a/0x260 [127.322583] ? __nf_unregister_net_hook+0x6a/0x260 [127.322590] ? __nf_tables_unregister_hook+0x8a/0xe0 [nf_tables] [127.322655] nft_table_disable+0x75/0xf0 [nf_tables] [127.322717] nf_tables_commit+0x2571/0x2620 [nf_tables]
CVE-20	5.8 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:H)	In the Linux kernel, the following vulnerability has been resolved: tcp: properly terminate timers for kernel sockets We had various syzbot reports about tcp timers firing after

24-35910		the corresponding netns has been dismantled. Fortunately Josef Bacik could trigger the issue more often, and could test a patch I wrote two years ago. When TCP sockets are closed, we call inet_csk_clear_xmit_timers() to 'stop' the timers. inet_csk_clear_xmit_timers() can be called from any context, including when socket lock is held. This is the reason it uses sk_stop_timer(), aka del_timer(). This means that ongoing timers might finish much later. For user sockets, this is fine because each running timer holds a reference on the socket, and the user socket holds a reference on the netns. For kernel sockets, we risk that the netns is freed before timer can complete, because kernel sockets do not hold reference on the netns. This patch adds inet_csk_clear_xmit_timers_sync() function that using sk_stop_timer_sync() to make sure all timers are terminated before the kernel socket is released. Modules using kernel sockets close them in their netns exit() handler. Also add sock_not_owned_by_me() helper to get LOCKDEP support : inet_csk_clear_xmit_timers_sync() must not be called while socket lock is held. It is very possible we can revert in the future commit 3a58f13a881e ("net: rds: acquire refcount on TCP sockets") which attempted to solve the issue in rds only. (net/smc/af_smc.c and net/mptcp/subflow.c have similar code) We probably can remove the check_net() tests from tcp_out_of_resources() and __tcp_close() in the future.
CVE-2024-3596	9.0 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H)	RADIUS Protocol under RFC 2865 is susceptible to forgery attacks by a local attacker who can modify any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response using a chosen-prefix collision attack against MD5 Response Authenticator signature.

CVE-2024-3651	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	A vulnerability was identified in the kjd/idna library, specifically within the `idna.encode()` function, affecting version 3.6. The issue arises from the function's handling of crafted input strings, which can lead to quadratic complexity and consequently, a denial of service condition. This vulnerability is triggered by a crafted input that causes the `idna.encode()` function to process the input with considerable computational load, significantly increasing the processing time in a quadratic manner relative to the input size.
CVE-2024-37370	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can modify the plaintext Extra Count field of a confidential GSS krb5 wrap token, causing the unwrapped token to appear truncated to the application.
CVE-2024-37371	9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)	In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can cause invalid memory reads during GSS message token handling by sending message tokens with invalid length fields.
CVE-2024-38822	2.7 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N)	Multiple methods in the salt master skip minion token validation. Therefore a misbehaving minion can impersonate another minion.

CVE-2024-38823	2.7 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N)	Salt's request server is vulnerable to replay attacks when not using a TLS encrypted transport.
CVE-2024-38824	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)	Directory traversal vulnerability in recv_file method allows arbitrary files to be written to the master cache directory.
CVE-2024-38825	6.4 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N)	The salt.auth.pki module does not properly authenticate callers. The "password" field contains a public certificate which is validated against a CA certificate by the module. This is not pki authentication, as the caller does not need access to the corresponding private key for the authentication attempt to be accepted.
CVE-2024-40906	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Always stop health timer during driver removal Currently, if teardown_hca fails to execute during driver removal, mlx5 does not stop the health timer. Afterwards, mlx5 continue with driver teardown. This may lead to a UAF bug, which results in page fault Oops[1], since the health timer invokes after resources were freed. Hence, stop the health monitor even if teardown_hca fails. [1] mlx5_core 0000:18:00.0: E-Switch: Unload vfs: mode(LEGACY), nvfs(0), necvfs(0), active vports(0) mlx5_core 0000:18:00.0: E-Switch: Disable: mode(LEGACY), nvfs(0), necvfs(0), active vports(0) mlx5_core 0000:18:00.0: E-Switch: Disable:

		mode(LEGACY), nvfs(0), necvfs(0), active vports(0) mlx5_core 0000:18:00.0: E-Switch: cleanup mlx5_core 0000:18:00.0: wait_func:1155:(pid 1967079): TEARDOWN_HCA(0x103) timeout. Will cause a leak of a command resource mlx5_core 0000:18:00.0: mlx5_function_close:1288:(pid 1967079): tear_down_hca failed, skip cleanup BUG: unable to handle page fault for address: ffffa26487064230 PGD 100c00067 P4D 100c00067 PUD 100e5a067 PMD 105ed7067 PTE 0 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 0 PID: 0 Comm: swapper/0 Tainted: G OE ------- --- 6.7.0-68.fc38.x86_64 #1 Hardware name: Intel Corporation S2600WFT/S2600WFT, BIOS SE5C620.86B.02.01.0013.121520200651 12/15/2020 RIP: 0010:ioread32be+0x34/0x60 RSP: 0018:ffffa26480003e58 EFLAGS: 00010292 RAX: ffffa26487064200 RBX: ffff9042d08161a0 RCX: ffff904c108222c0 RDX: 000000010bbf1b80 RSI: ffffffffc055ddb0 RDI: ffffa26487064230 RBP: ffff9042d08161a0 R08: 0000000000000022 R09: ffff904c108222e8 R10: 0000000000000004 R11: 0000000000000441 R12: ffffffffc055ddb0 R13: ffffa26487064200 R14: ffffa26480003f00 R15: ffff904c108222c0 FS: 0000000000000000(0000) GS:ffff904c10800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffa26487064230 CR3: 00000002c4420006 CR4: 00000000007706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <IRQ> ? __die+0x23/0x70 ? page_fault_oops+0x171/0x4e0 ? exc_page_fault+0x175/0x180 ? asm_exc_page_fault+0x26/0x30 ? __pfx_poll_health+0x10/0x10 [mlx5_core] ? __pfx_poll_health+0x10/0x10 [mlx5_core] ? ioread32be+0x34/0x60 mlx5_health_check_fatal_sensors+0x20/0x100

		[mlx5_core] ? __pfx_poll_health+0x10/0x10 [mlx5_core] poll_health+0x42/0x230 [mlx5_core] ? __next_timer_interrupt+0xbc/0x110 ? __pfx_poll_health+0x10/0x10 [mlx5_core] call_timer_fn+0x21/0x130 ? __pfx_poll_health+0x10/0x10 [mlx5_core] __run_timers+0x222/0x2c0 run_timer_softirq+0x1d/0x40 __do_softirq+0xc9/0x2c8 __irq_exit_rcu+0xa6/0xc0 sysvec_apic_timer_interrupt+0x72/0x90 </IRQ> <TASK> asm_sysvec_apic_timer_interrupt+0x1a/0x20 RIP: 0010:cpuidle_enter_state+0xcc/0x440 ? cpuidle_enter_state+0xbd/0x440 cpuidle_enter+0x2d/0x40 do_idle+0x20d/0x270 cpu_startup_entry+0x2a/0x30 rest_init+0xd0/0xd0 arch_call_rest_init+0xe/0x30 start_kernel+0x709/0xa90 x86_64_start_reservations+0x18/0x30 x86_64_start_kernel+0x96/0xa0 secondary_startup_64_no_verify+0x18f/0x19b ---[end trace 0000000000000000]---
CVE-2024-43842	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: Fix array index mistake in rtw89_sta_info_get_iter() In rtw89_sta_info_get_iter() 'status->he_gi' is compared to array size. But then 'rate->he_gi' is used as array index instead of 'status->he_gi'. This can lead to go beyond array boundaries in case of 'rate->he_gi' is not equal to 'status->he_gi' and is bigger than array size. Looks like "copy-paste" mistake. Fix this mistake by replacing 'rate->he_gi' with 'status->he_gi'. Found by Linux Verification Center (linuxtesting.org) with SVACE.
CVE-2024-44	5.5 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: SHAMPO, Fix invalid WQ linked list unlink When all the strides in a WQE have been consumed, the WQE is unlinked from the WQ linked list (mlx5_wq_ll_pop()). For SHAMPO, it is possible to receive

970		CQEs with 0 consumed strides for the same WQE even after the WQE is fully consumed and unlinked. This triggers an additional unlink for the same wqe which corrupts the linked list. Fix this scenario by accepting 0 sized consumed strides without unlinking the WQE again.
CVE-2024-45802	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	Squid is an open source caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to Input Validation, Premature Release of Resource During Expected Lifetime, and Missing Release of Resource after Effective Lifetime bugs, Squid is vulnerable to Denial of Service attacks by a trusted server against all clients using the proxy. This bug is fixed in the default build configuration of Squid version 6.10.
CVE-2024-5314 1	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: add missing range check in bitmap_ip_uadt When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists, the values of ip and ip_to are slightly swapped. Therefore, the range check for ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks.
CVE-2024-5535	9.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H)	Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash. In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario

		and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a "no overlap" response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a

		protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available.
CVE-2024-5554 9	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	xsltGetInheritedNsList in libxslt before 1.1.43 has a use-after-free issue related to exclusion of result prefixes.
CVE-2024-5564	8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	A vulnerability was found in libndp. This flaw allows a local malicious user to cause a buffer overflow in NetworkManager, triggered by sending a malformed IPv6 router advertisement packet. This issue occurred as libndp was not correctly validating the route length information.

CVE-2024-56171	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a use-after-free in xmlSchemaIDCFillNodeTables and xmlSchemaBubbleIDCNodeTables in xmlschemas.c. To exploit this, a crafted XML document must be validated against an XML schema with certain identity constraints, or a crafted XML schema must be used.
CVE-2024-56326	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	Jinja is an extensible templating engine. Prior to 3.1.5, An oversight in how the Jinja sandboxed environment detects calls to str.format allows an attacker that controls the content of a template to execute arbitrary Python code. To exploit the vulnerability, an attacker needs to control the content of a template. Whether that is the case depends on the type of application using Jinja. This vulnerability impacts users of applications which execute untrusted templates. Jinja's sandbox does catch calls to str.format and ensures they don't escape the sandbox. However, it's possible to store a reference to a malicious string's format method, then pass that to a filter that calls it. No such filters are built-in to Jinja, but could be present through custom filters in an application. After the fix, such indirect calls are also handled by the sandbox. This vulnerability is fixed in 3.1.5.
CVE-2024-6232	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	There is a MEDIUM severity vulnerability affecting CPython. Regular expressions that allowed excessive backtracking during tarfile.TarFile header parsing are vulnerable to ReDoS via specifically-crafted tar archives.
CVE-2024-	4.7 (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_mp4_module, which might allow an attacker to over-read NGINX worker memory resulting in its termination, using a specially crafted mp4 file. The issue only affects NGINX if it is built with the

7347		ngx_http_mp4_module and the mp4 directive is used in the configuration file. Additionally, the attack is possible only if an attacker can trigger the processing of a specially crafted mp4 file with the ngx_http_mp4_module. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.
CVE-2024-9143	4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)	Issue summary: Use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes. Impact summary: Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only "named curves" are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary (GF(2^m)) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low. In particular, the X9.62 encoding is used for ECC keys in X.509 certificates, so problematic inputs cannot occur in the context of processing X.509 certificates. Any problematic use-cases would have to be using an "exotic" curve encoding. The affected APIs include: EC_GROUP_new_curve_GF2m(), EC_GROUP_new_from_params(), and various supporting BN_GF2m_*() functions. Applications working with "exotic" explicit binary (GF(2^m)) curve parameters, that make it possible to represent invalid field polynomials with a zero constant term, via the above or similar APIs, may terminate abruptly as a result of reading or writing outside of array bounds. Remote code execution cannot easily be ruled out. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.
CVE-20	7.6 (CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H)	A flaw was found in grub2. During the network boot process, when trying to search for the configuration file, grub copies data from a user controlled environment

25-06-24		variable into an internal buffer using the grub_strcpy() function. During this step, it fails to consider the environment variable length when allocating the internal buffer, resulting in an out-of-bounds write. If correctly exploited, this issue may result in remote code execution through the same network segment grub is searching for the boot information, which can be used to by-pass secure boot protections.
CVE-2025-21587	7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE:8u441, 8u441-perf, 11.0.26, 17.0.14, 21.0.6, 24; Oracle GraalVM for JDK:17.0.14, 21.0.6, 24; Oracle GraalVM Enterprise Edition:20.3.17 and 21.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).

CVE-2025-21589		An Authentication Bypass Using an Alternate Path or Channel vulnerability in Juniper Networks Session Smart Router may allows a network-based attacker to bypass authentication and take administrative control of the device. This issue affects Session Smart Router: * from 5.6.7 before 5.6.17, * from 6.0 before 6.0.8 (affected from 6.0.8), * from 6.1 before 6.1.12-lts, * from 6.2 before 6.2.8-lts, * from 6.3 before 6.3.3-r2; This issue affects Session Smart Conductor: * from 5.6.7 before 5.6.17, * from 6.0 before 6.0.8 (affected from 6.0.8), * from 6.1 before 6.1.12-lts, * from 6.2 before 6.2.8-lts, * from 6.3 before 6.3.3-r2; This issue affects WAN Assurance Managed Routers: * from 5.6.7 before 5.6.17, * from 6.0 before 6.0.8 (affected from 6.0.8), * from 6.1 before 6.1.12-lts, * from 6.2 before 6.2.8-lts, * from 6.3 before 6.3.3-r2.
CVE-2025-21756	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	In the Linux kernel, the following vulnerability has been resolved: vsock: Keep the binding until socket destruction Preserve sockets bindings; this includes both resulting from an explicit bind() and those implicitly bound through autobind during connect(). Prevents socket unbinding during a transport reassignment, which fixes a use-after-free: 1. vsock_create() (refcnt=1) calls vsock_insert_unbound() (refcnt=2) 2. transport->release() calls vsock_remove_bound() without checking if sk was bound and moved to bound list (refcnt=1) 3. vsock_bind() assumes sk is in unbound list and before __vsock_insert_bound(vsock_bound_sockets()) calls __vsock_remove_bound() which does: list_del_init(&vsk->bound_table); // nop sock_put(&vsk->sk); // refcnt=0 BUG: KASAN: slab-use-after-free in __vsock_bind+0x62e/0x730 Read of size 4 at addr ffff88816b46a74c by task a.out/2057 dump_stack_lvl+0x68/0x90 print_report+0x174/0x4f6 kasan_report+0xb9/0x190 __vsock_bind+0x62e/0x730 vsock_bind+0x97/0xe0 __sys_bind+0x154/0x1f0

		__x64_sys_bind+0x6e/0xb0 do_syscall_64+0x93/0x1b0 entry_SYSCALL_64_after_hwframe+0x76/0x7e Allocated by task 2057: kasan_save_stack+0x1e/0x40 kasan_save_track+0x10/0x30 __kasan_slab_alloc+0x85/0x90 kmem_cache_alloc_noprof+0x131/0x450 sk_prot_alloc+0x5b/0x220 sk_alloc+0x2c/0x870 __vsock_create.constprop.0+0x2e/0xb60 vsock_create+0xe4/0x420 __sock_create+0x241/0x650 __sys_socket+0xf2/0x1a0 __x64_sys_socket+0x6e/0xb0 do_syscall_64+0x93/0x1b0 entry_SYSCALL_64_after_hwframe+0x76/0x7e Freed by task 2057: kasan_save_stack+0x1e/0x40 kasan_save_track+0x10/0x30 kasan_save_free_info+0x37/0x60 __kasan_slab_free+0x4b/0x70 kmem_cache_free+0x1a1/0x590 __sk_destruct+0x388/0x5a0 __vsock_bind+0x5e1/0x730 vsock_bind+0x97/0xe0 __sys_bind+0x154/0x1f0 __x64_sys_bind+0x6e/0xb0 do_syscall_64+0x93/0x1b0 entry_SYSCALL_64_after_hwframe+0x76/0x7e refcount_t: addition on 0; use-after-free. WARNING: CPU: 7 PID: 2057 at lib/refcount.c:25 refcount_warn_saturate+0xce/0x150 RIP: 0010:refcount_warn_saturate+0xce/0x150 __vsock_bind+0x66d/0x730 vsock_bind+0x97/0xe0 __sys_bind+0x154/0x1f0 __x64_sys_bind+0x6e/0xb0 do_syscall_64+0x93/0x1b0 entry_SYSCALL_64_after_hwframe+0x76/0x7e refcount_t: underflow; use-after-free. WARNING: CPU: 7 PID: 2057 at lib/refcount.c:28 refcount_warn_saturate+0xee/0x150 RIP: 0010:refcount_warn_saturate+0xee/0x150 vsock_remove_bound+0x187/0x1e0 __vsock_release+0x383/0x4a0 vsock_release+0x90/0x120 __sock_release+0xa3/0x250 sock_close+0x14/0x20 __fput+0x359/0xa80 task_work_run+0x107/0x1d0 do_exit+0x847/0x2560 do_group_exit+0xb8/0x250 __x64_sys_exit_group+0x3a/0x50

		x64_sys_call+0xfec/0x14f0 do_syscall_64+0x93/0x1b0 entry_SYSCALL_64_after_hwframe+0x76/0x7e
CVE-2025-22236	8.1 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L)	Minion event bus authorization bypass. An attacker with access to a minion key can craft a message which may be able to execute a job on other minions (>= 3007.0).
CVE-2025-22237	6.7 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H)	An attacker with access to a minion key can exploit the 'on demand' pillar functionality with a specially crafted git url which could cause and arbitrary command to be run on the master with the same privileges as the master process.
CVE-2025-22238	4.2 (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N)	Directory traversal attack in minion file cache creation. The master's default cache is vulnerable to a directory traversal attack. Which could be leveraged to write or overwrite 'cache' files outside of the cache directory.
CVE-2025-22239	8.1 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L)	Arbitrary event injection on Salt Master. The master's "_minion_event" method can be used by and authorized minion to send arbitrary events onto the master's event bus.

CVE-2025-22240	6.3 (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H)	Arbitrary directory creation or file deletion. In the find_file method of the GitFS class, a path is created using os.path.join using unvalidated input from the “tgt_env” variable. This can be exploited by an attacker to delete any file on the Master's process has permissions to.
CVE-2025-22241	5.6 (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:N)	File contents overwrite the VirtKey class is called when “on-demand pillar” data is requested and uses un-validated input to create paths to the “pki directory”. The functionality is used to auto-accept Minion authentication keys based on a pre-placed “authorization file” at a specific location and is present in the default configuration.
CVE-2025-22242	5.6 (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:N/A:H)	Worker process denial of service through file read operation. .A vulnerability exists in the Master's “pub_ret” method which is exposed to all minions. The un-sanitized input value “jid” is used to construct a path which is then opened for reading. An attacker could exploit this vulnerabilities by attempting to read from a filename that will not return any data, e.g. by targeting a pipe node on the proc file system.
CVE-2025-23419	4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)	When multiple server blocks are configured to share the same IP address and port, an attacker can use session resumption to bypass client certificate authentication requirements on these servers. This vulnerability arises when TLS Session Tickets https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_ticket_key are used and/or the SSL session cache https://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_session_cache are used in the default server and the default server is performing client certificate authentication. Note: Software versions which have

		reached End of Technical Support (EoTS) are not evaluated.
CVE-2025-24528		
CVE-2025-24855	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	numbers.c in libxslt before 1.1.43 has a use-after-free because, in nested XPath evaluations, an XPath context node can be modified but never restored. This is related to xsltNumberFormatGetValue, xsltEvalXPathPredicate, xsltEvalXPathStringNs, and xsltComputeSortResultInternal.
CVE-2025-24928	7.7 (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N)	libxml2 before 2.12.10 and 2.13.x before 2.13.6 has a stack-based buffer overflow in xmlSnprintfElements in valid.c. To exploit this, DTD validation must occur for an untrusted document or untrusted DTD. NOTE: this is similar to CVE-2017-9047.
CVE-2025-27363	8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	An out of bounds write exists in FreeType versions 2.13.0 and below (newer versions of FreeType are not vulnerable) when attempting to parse font subglyph structures related to TrueType GX and variable font files. The vulnerable code assigns a signed short value to an unsigned long and then adds a static value causing it to wrap around and allocate too small of a heap buffer. The code then writes up to 6 signed long integers out of bounds relative to this buffer. This may result in arbitrary

		code execution. This vulnerability may have been exploited in the wild.
CVE-2025-29087	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	In SQLite 3.44.0 through 3.49.0 before 3.49.1, the concat_ws() SQL function can cause memory to be written beyond the end of a malloc-allocated buffer. If the separator argument is attacker-controlled and has a large string (e.g., 2MB or more), an integer overflow occurs in calculating the size of the result buffer, and thus malloc may not allocate enough memory.
CVE-2025-30691	4.8 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)	Vulnerability in Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle Java SE: 21.0.6, 24; Oracle GraalVM for JDK: 21.0.6 and 24. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data as well as unauthorized read access to a subset of Oracle Java SE accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2025-30	5.6 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u441, 8u441-perf, 11.0.26, 17.0.14, 21.0.6, 24; Oracle GraalVM for JDK: 17.0.14, 21.0.6, 24; Oracle GraalVM Enterprise Edition: 20.3.17 and

698		21.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L).
CVE-2025-30749	8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java

		deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2025-30754	4.8 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).

CVE-2025-30761	5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Scripting). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf and 11.0.27; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2025-48002	7.8 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)	Untrusted LD_LIBRARY_PATH environment variable vulnerability in the GNU C Library version 2.27 to 2.38 allows attacker controlled loading of dynamically shared library in statically compiled setuid binaries that call dlopen (including internal dlopen calls after setlocale or calls to NSS functions such as getaddrinfo).
CVE-2025-49844	9.9 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)	Redis is an open source, in-memory database that persists on disk. Versions 8.2.1 and below allow an authenticated user to use a specially crafted Lua script to manipulate the garbage collector, trigger a use-after-free and potentially lead to remote code execution. The problem exists in all versions of Redis with Lua scripting. This issue is fixed in version 8.2.2. To workaround this issue without patching the redis-server executable is to prevent users from

		executing Lua scripts. This can be done using ACL to restrict EVAL and EVALSHA commands.
CVE-2025-501066	8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 8u451, 8u451-perf, 11.0.27, 17.0.15, 21.0.7, 24.0.1; Oracle GraalVM for JDK: 17.0.15, 21.0.7 and 24.0.1; Oracle GraalVM Enterprise Edition: 21.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in takeover of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2025-6020	7.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)	A flaw was found in linux-pam. The module pam_namespace may use access user-controlled paths without proper protection, allowing local users to elevate their privileges to root via multiple symlink attacks and race conditions.
CVE-20	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	There exists a vulnerability in SQLite versions before 3.50.2 where the number of aggregate terms could exceed the number of columns available. This could lead to a

25-6965		memory corruption issue. We recommend upgrading to version 3.50.2 or above.
CVE-2025-7425	7.8 (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:H)	A flaw was found in libxslt where the attribute type, atype, flags are modified in a way that corrupts internal memory management. When XSLT functions, such as the key() process, result in tree fragments, this corruption prevents the proper cleanup of ID attributes. As a result, the system may access freed memory, causing crashes or enabling attackers to trigger heap corruption.

Impact:

Exploits:

Juniper SIRT is not aware of any malicious exploitation of these vulnerabilities.

This issue was discovered by a third-party upstream provider.

Product Status:

Product	Affected
Juniper Networks Session Smart Router	All versions before 6.2.10-lts
Default status is affected	from 6.3.0 before 6.3.6-sts

Solution:

The following software releases have been updated to resolve these specific issues:

Session Smart Router: 6.2.10-lts, and all subsequent 6.2 releases, 6.3.6-sts, and all subsequent 6.3 releases.

This issue is being tracked as I95-62825 I95-62360 I95-62356 I95-62355 I95-62353 I95-62107 I95-61569 I95-61555 I95-61482 I95-61481 I95-61476 I95-61159 I95-61156 I95-61153 I95-61152 I95-60793 I95-60792 I95-60790 I95-60788 I95-60787 I95-60785 I95-60784 I95-60783 I95-60781 I95-60780 I95-60778 I95-60288 I95-59677 I95-58522 I95-58521 I95-58356 I95-58355 I95-57778 I95-57611 I95-57214 I95-57111 I95-57054 I95-57053 I95-56496 I95-56409 I95-56065 I95-55799

I95-55628 I95-55627 I95-55626 I95-55624 I95-55622 I95-55401 I95-54994 I95-54748 I95-54623 I95-54362 I95-54302 I95-54048 I95-54027 I95-54026 I95-53838 I95-53817 I95-53797 I95-53622 I95-53477 I95-53476 I95-52956 I95-52645 I95-52644 I95-52625 I95-52554 I95-52509 I95-52497 I95-52496 I95-52495 I95-51758 I95-51431 I95-50790 I95-50523 I95-50508 I95-50359 I95-50358 which is visible on the Customer Support website.Note: Juniper SIRT's policy is not to evaluate releases which are beyond End of Engineering (EOE) or End of Life (EOL).

Workaround:

There are no known workarounds for these issues.

Internal Comments:

Note to Support: If Problem section states 'Juniper SIRT is not aware of any malicious exploitation ...' and if you come across a case or customer enquiry that may indicate malicious exploitation of the issue, please bring it to the attention of SIRT sirt@juniper.net immediately.

CVSS ASSESSMENT:

CVSS: v3.1: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) CVSS: v4.0: 9.9 (CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:H/V:C/RE:M/U:Amber)