CVE	Description
CVE-2022-42703	mm/rmap.c in the Linux kernel before 5.19.7 has a use-after-free related to leaf anon_vma double reuse.
CVE-2022-40307	An issue was discovered in the Linux kernel through 5.19.8. drivers/firmware/efi/capsule-loader.c has a race condition with a resultant use-after-free.
CVE-2022-39188	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-2022-42328	Guests can trigger deadlock in Linux netback driver T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] The patch for XSA-392 introduced another issue which might result in a deadlock when trying to free the SKB of a packet dropped due to the XSA-392 handling (CVE-2022-42328). Additionally when dropping packages for other reasons the same deadlock could occur in case of netpoll being active for the interface the xen-netback driver is connected to (CVE-2022-42329).
CVE-2022-42329	Guests can trigger deadlock in Linux netback driver T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] The patch for XSA-392 introduced another issue which might result in a deadlock when trying to free the SKB of a packet dropped due to the XSA-392 handling (CVE-2022-42328). Additionally when dropping packages for other reasons the same deadlock could occur in case of netpoll being active for the interface the xen-netback driver is connected to (CVE-2022-42329).
CVE-2023-0394	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-2022-32296	The Linux kernel before 5.17.9 allows TCP servers to identify clients by observing what source ports are used. This occurs because of use of Algorithm 4 (“Double-Hash Port Selection Algorithm”) of RFC 6056.
CVE-2022-41849	drivers/video/fbdev/smscufx.c in the Linux kernel through 5.19.12 has a race condition and resultant use-after-free if a physically proximate attacker removes a USB device while calling open(), aka a race condition between ufx_ops_open and ufx_usb_disconnect.
CVE-2022-1012	A memory leak problem was found in the TCP source port generation algorithm in net/ipv4/tcp.c due to the small table perturb size. This flaw may allow an attacker to information leak and may cause a denial of service problem.
CVE-2022-3028	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-2022-41222	mm/mremap.c in the Linux kernel before 5.13.3 has a use-after-free via a stale TLB because an rmap lock is not held during a PUD move.
CVE-2022-43945	The Linux kernel NFSD implementation prior to versions 5.19.17 and 6.0.2 are vulnerable to buffer overflow. NFSD tracks the number of pages held by each NFSD thread by combining the receive and send buffers of a remote procedure call (RPC) into a single array of pages. A client can force the send buffer to shrink by sending an RPC message over TCP with garbage data added at the end of the message. The RPC message with garbage data is still correctly formed according to the specification and is passed forward to handlers. Vulnerable code in NFSD is not expecting the oversized request and writes beyond the allocated buffer space. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVE-2022-2503	Dm-verity is used for extending root-of-trust to root filesystems. LoadPin builds on this property to restrict module/firmware loads to just the trusted root filesystem. Device-mapper table reloads currently allow users with root privileges to switch out the target with an equivalent dm-linear target and bypass verification till reboot. This allows root to bypass LoadPin and can be used to load untrusted and unverified kernel modules and firmware, which implies arbitrary kernel execution and persistence for peripherals that do not verify firmware updates. We recommend upgrading past commit 4caae58406f8ceb741603eee460d79bacca9b1b5
CVE-2022-2196	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-2021-39537	An issue was discovered in ncurses through v6.2-1. _nc_captoinfo in captoinfo.c has a heap-based buffer overflow.
CVE-2022-29458	ncurses 6.3 before patch 20220416 has an out-of-bounds read and segmentation violation in convert_strings in tinfo/read_entry.c in the terminfo library.