# SSA-794697: Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 TM MFP before V1.1

| | |
|---|---|
| Publication Date: | 2023-06-13 |
| Last Update: | 2024-04-09 |
| Current Version: | V1.8 |
| CVSS v3.1 Base Score: | 9.8 |
| CVSS v4.0 Base Score: | 8.2 |

## SUMMARY

Multiple vulnerabilities have been identified in the additional GNU/Linux subsystem of the SIMATIC S7-1500 TM MFP V1.0.

Siemens has released a new version for SIMATIC S7-1500 TM MFP - GNU/Linux subsystem and recommends to update to the latest version.

This advisory lists vulnerabilities for firmware version V1.0 only; for V1.1 refer to Siemens Security Advisory SSA-265688 (https://cert-portal.siemens.com/productcert/html/ssa-265688.html).

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SIMATIC S7-1500 TM MFP - GNU/Linux subsystem:<br>All versions < V1.1<br>affected by all CVEs | Update to V1.1 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109827684/<br>See further recommendations from section Workarounds and Mitigations |

## WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Only build and run applications from trusted sources

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

## GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

## PRODUCT DESCRIPTION

SIMATIC S7-1500 TM MFP is a Technology module Multi functional platform for SIMATIC S7-1500 PLCs based on SIMATIC Industrial OS

## VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

### Vulnerability CVE-2020-12762

json-c through 0.14 has an integer overflow and out-of-bounds write via a large JSON file, as demonstrated by printbuf_memappend.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-190: Integer Overflow or Wraparound |

### Vulnerability CVE-2021-3759

A memory overflow vulnerability was found in the Linux kernel's ipc functionality of the memcg subsystem, in the way a user calls the semget function multiple times, creating semaphores. This flaw allows a local user to starve the resources, causing a denial of service. The highest threat from this vulnerability is to system availability.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-400: Uncontrolled Resource Consumption |

### Vulnerability CVE-2021-4037

A vulnerability was found in the fs/inode.c:inode_init_owner() function logic of the LInux kernel that allows local users to create files for the XFS file-system with an unintended group ownership and with group execution and SGID permission bits set, in a scenario where a directory is SGID and belongs to a certain group and is writable by a user who is not a member of this group. This can lead to excessive permissions granted in case when they should not. This vulnerability is similar to the previous CVE-2018-13405 and adds the missed fix for the XFS.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-284: Improper Access Control |

### Vulnerability CVE-2021-33655

When sending malicous data to kernel by ioctl cmd FBIOPUT_VSCREENINFO,kernel will write memory out of bounds.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2021-44879

In gc_data_segment in fs/f2fs/gc.c in the Linux kernel before 5.16.3, special files are not considered, leading to a move_data_page NULL pointer dereference.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2022-0171

A flaw was found in the Linux kernel. The existing KVM SEV API has a vulnerability that allows a non-root (host) user-level application to crash the host kernel by creating a confidential guest VM instance in AMD CPU that supports Secure Encrypted Virtualization (SEV).

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-459: Incomplete Cleanup |

### Vulnerability 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.

| | |
|---|---|
| CVSS v3.1 Base Score | 8.2 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-401: Missing Release of Memory after Effective Lifetime |

### Vulnerability CVE-2022-1015

A flaw was found in the Linux kernel in linux/net/netfilter/nf_tables_api.c of the netfilter subsystem. This flaw allows a local user to cause an out-of-bounds write issue.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.6 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2022-1184

A use-after-free flaw was found in fs/ext4/namei.c:dx_insert_block() in the Linux kernel's filesystem sub-component. This flaw allows a local attacker with a user privilege to cause a denial of service.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-1292

The c_rehash script does not properly sanitise shell metacharacters to prevent command injection.

| | |
|---|---|
| CVSS v3.1 Base Score | 9.8 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |

### Vulnerability CVE-2022-1343

Under certain circumstances, the command line OCSP verify function reports successful verification when the verification in fact failed. In this case the incorrect successful response will also be accompanied by error messages showing the failure and contradicting the apparently successful result.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C |
| CWE | CWE-295: Improper Certificate Validation |

### Vulnerability CVE-2022-1434

When using the RC4-MD5 ciphersuite, which is disabled by default, an attacker is able to modify data in transit due to an incorrect use of the AAD data as the MAC key in OpenSSL 3.0. An attacker is not able to decrypt any communication.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.9 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C |
| CWE | CWE-327: Use of a Broken or Risky Cryptographic Algorithm |

### Vulnerability CVE-2022-1462

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.3 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |

### Vulnerability CVE-2022-1473

The used OpenSSL version improperly reuses memory when decoding certificates or keys. This can lead to a process termination and Denial of Service for long lived processes.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-404: Improper Resource Shutdown or Release |

### Vulnerability CVE-2022-1679

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-1852

A NULL pointer dereference flaw was found in the Linux kernel's KVM module, which can lead to a denial of service in the x86_emulate_insn in arch/x86/kvm/emulate.c. This flaw occurs while executing an illegal instruction in guest in the Intel CPU.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2022-1882

A use-after-free flaw was found in the Linux kernel's pipes functionality in how a user performs manipulations with the pipe post_one_notification() after free_pipe_info() that is already called. This flaw allows a local user to crash or potentially escalate their privileges on the system.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

## Vulnerability CVE-2022-2068

In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.

| | |
|---|---|
| CVSS v3.1 Base Score | 9.8 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |

## Vulnerability CVE-2022-2078

A vulnerability was found in the Linux kernel's nft_set_desc_concat_parse() function .This flaw allows an attacker to trigger a buffer overflow via nft_set_desc_concat_parse() , causing a denial of service and possibly to run code.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-121: Stack-based Buffer Overflow |

## Vulnerability CVE-2022-2097

AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-326: Inadequate Encryption Strength |

## Vulnerability CVE-2022-2153

A flaw was found in the Linux kernel's KVM when attempting to set a SynIC IRQ. This issue makes it possible for a misbehaving VMM to write to SYNIC/STIMER MSRs, causing a NULL pointer dereference. This flaw allows an unprivileged local attacker on the host to issue specific ioctl calls, causing a kernel oops condition that results in a denial of service.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2022-2274

The OpenSSL 3.0.4 release introduced a serious bug in the RSA implementation for X86_64 CPUs supporting the AVX512IFMA instructions. This issue makes the RSA implementation with 2048 bit private keys incorrect on such machines and memory corruption will happen during the computation. As a consequence of the memory corruption an attacker may be able to trigger a remote code execution on the machine performing the computation. SSL/TLS servers or other servers using 2048 bit RSA private keys running on machines supporting AVX512IFMA instructions of the X86_64 architecture are affected by this issue.

| | |
|---|---|
| CVSS v3.1 Base Score | 9.8 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2022-2327

io_uring use work_flags to determine which identity need to grab from the calling process to make sure it is consistent with the calling process when executing IORING_OP. Some operations are missing some types, which can lead to incorrect reference counts which can then lead to a double free. We recommend upgrading the kernel past commit df3f3bb5059d20ef094d6b2f0256c4bf4127a859

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-415: Double Free |

### Vulnerability 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

| | |
|---|---|
| CVSS v3.1 Base Score | 6.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-287: Improper Authentication |

### Vulnerability CVE-2022-2586

A use-after-free flaw was found in nf_tables cross-table in the net/netfilter/nf_tables_api.c function in the Linux kernel. This flaw allows a local, privileged attacker to cause a use-after-free problem at the time of table deletion, possibly leading to local privilege escalation.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-2588

Zhenpeng Lin discovered that the network packet scheduler implementation in the Linux kernel did not properly remove all references to a route filter before freeing it in some situations. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2022-2602

A flaw was found in the Linux kernel. A race issue occurs between an io_uring request and the Unix socket garbage collector, allowing an attacker local privilege escalation.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.0 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2022-2663

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C |
| CWE | CWE-923: Improper Restriction of Communication Channel to Intended Endpoints |

### Vulnerability CVE-2022-2905

An out-of-bounds memory read flaw was found in the Linux kernel's BPF subsystem in how a user calls the bpf_tail_call function with a key larger than the max_entries of the map. This flaw allows a local user to gain unauthorized access to data.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2022-2959

A race condition was found in the Linux kernel's watch queue due to a missing lock in pipe_resize_ring(). The specific flaw exists within the handling of pipe buffers. The issue results from the lack of proper locking when performing operations on an object. This flaw allows a local user to crash the system or escalate their privileges on the system.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.0 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |

### Vulnerability CVE-2022-2978

A flaw use after free in the Linux kernel NILFS file system was found in the way user triggers function security_inode_alloc to fail with following call to function nilfs_mdt_destroy. A local user could use this flaw to crash the system or potentially escalate their privileges on the system.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability 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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.0 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |

### Vulnerability CVE-2022-3104

An issue was discovered in the Linux kernel through 5.16-rc6. lkdtm_ARRAY_BOUNDS in drivers/misc/lkdtm/bugs.c lacks check of the return value of kmalloc() and will cause the null pointer dereference.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2022-3115

An issue was discovered in the Linux kernel through 5.16-rc6. malidp_crtc_reset in drivers/gpu/drm/arm/malidp_crtc.c lacks check of the return value of kzalloc() and will cause the null pointer dereference.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2022-3169

A flaw was found in the Linux kernel. A denial of service flaw may occur if there is a consecutive request of the NVME_IOCTL_RESET and the NVME_IOCTL_SUBSYS_RESET through the device file of the driver, resulting in a PCIe link disconnect.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2022-3303

A race condition flaw was found in the Linux kernel sound subsystem due to improper locking. It could lead to a NULL pointer dereference while handling the SNDCTL_DSP_SYNC ioctl. A privileged local user (root or member of the audio group) could use this flaw to crash the system, resulting in a denial of service condition

| | |
|---|---|
| CVSS v3.1 Base Score | 4.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |

### Vulnerability CVE-2022-3521

A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function kcm_tx_work of the file net/kcm/kcmsock.c of the component kcm. The manipulation leads to race condition. It is recommended to apply a patch to fix this issue. VDB-211018 is the identifier assigned to this vulnerability.

| | |
|---|---|
| CVSS v3.1 Base Score | 2.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C |
| CWE | CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |

### Vulnerability CVE-2022-3524

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-404: Improper Resource Shutdown or Release |

### Vulnerability CVE-2022-3534

A vulnerability classified as critical has been found in Linux Kernel. Affected is the function btf_dump_name_dups of the file tools/lib/bpf/btf_dump.c of the component libbpf. 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-211032.

| | |
|---|---|
| CVSS v3.1 Base Score | 8.0 |
| CVSS Vector | CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-3545

A vulnerability has been found in Linux Kernel and classified as critical. Affected by this vulnerability is the function area_cache_get of the file drivers/net/ethernet/netronome/nfp/nfpcore/nfp_cppcore.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-211045 was assigned to this vulnerability.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |

### Vulnerability CVE-2022-3564

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.1 |
| CVSS Vector | CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |

### Vulnerability CVE-2022-3565

A vulnerability, which was classified as critical, has been found in Linux Kernel. Affected by this issue is the function del_timer of the file drivers/isdn/mISDN/l1oip_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-211088.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |

### Vulnerability CVE-2022-3586

A flaw was found in the Linux kernel's networking code. A use-after-free was found in the way the sch_sfb enqueue function used the socket buffer (SKB) cb field after the same SKB had been enqueued (and freed) into a child qdisc. This flaw allows a local, unprivileged user to crash the system, causing a denial of service.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-3594

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C |
| CWE | CWE-404: Improper Resource Shutdown or Release |

### Vulnerability CVE-2022-3606

A vulnerability was found in Linux Kernel. It has been classified as problematic. This affects the function find_prog_by_sec_insn of the file tools/lib/bpf/libbpf.c of the component BPF. The manipulation leads to null pointer dereference. It is recommended to apply a patch to fix this issue. The identifier VDB-211749 was assigned to this vulnerability.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2022-3621

A vulnerability was found in Linux Kernel. It has been classified as problematic. Affected is the function nilfs_bmap_lookup_at_level of the file fs/nilfs2/inode.c of the component nilfs2. The manipulation leads to null pointer dereference. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211920.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2022-3625

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |

### Vulnerability CVE-2022-3628

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.6 |
| CVSS Vector | CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') |

### Vulnerability CVE-2022-3629

A vulnerability was found in Linux Kernel. It has been declared as problematic. This vulnerability affects the function vsock_connect of the file net/vmw_vsock/af_vsock.c. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. VDB-211930 is the identifier assigned to this vulnerability.

| | |
|---|---|
| CVSS v3.1 Base Score | 3.3 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C |
| CWE | CWE-401: Missing Release of Memory after Effective Lifetime |

### Vulnerability CVE-2022-3633

A vulnerability classified as problematic has been found in Linux Kernel. Affected is the function j1939_session_destroy of the file net/can/j1939/transport.c. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211932.

| | |
|---|---|
| CVSS v3.1 Base Score | 3.3 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C |
| CWE | CWE-401: Missing Release of Memory after Effective Lifetime |

### Vulnerability CVE-2022-3635

A vulnerability, which was classified as critical, has been found in Linux Kernel. Affected by this issue is the function tst_timer of the file drivers/atm/idt77252.c of the component IPsec. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. VDB-211934 is the identifier assigned to this vulnerability.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.0 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |

### Vulnerability CVE-2022-3646

A vulnerability, which was classified as problematic, has been found in Linux Kernel. This issue affects the function nilfs_attach_log_writer of the file fs/nilfs2/segment.c of the component BPF. The manipulation leads to memory leak. The attack may be initiated remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211961 was assigned to this vulnerability.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C |
| CWE | CWE-404: Improper Resource Shutdown or Release |

### Vulnerability CVE-2022-3649

A vulnerability was found in Linux Kernel. It has been classified as problematic. Affected is the function nilfs_new_inode of the file fs/nilfs2/inode.c of the component BPF. The manipulation leads to use after free. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211992.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer |

### Vulnerability CVE-2022-4095

A use-after-free flaw was found in Linux kernel before 5.19.2. This issue occurs in cmd_hdl_filter in drivers/staging/rtl8712/rtl8712_cmd.c, allowing an attacker to launch a local denial of service attack and gain escalation of privileges.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-4129

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-667: Improper Locking |

### Vulnerability CVE-2022-4139

An incorrect TLB flush issue was found in the Linux kernel's GPU i915 kernel driver, potentially leading to random memory corruption or data leaks. This flaw could allow a local user to crash the system or escalate their privileges on the system.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-401: Missing Release of Memory after Effective Lifetime |

## Vulnerability CVE-2022-4269

A flaw was found in the Linux kernel Traffic Control (TC) subsystem. Using a specific networking configuration (redirecting egress packets to ingress using TC action “mirred") a local unprivileged user could trigger a CPU soft lockup (ABBA deadlock) when the transport protocol in use (TCP or SCTP) does a retransmission, resulting in a denial of service condition.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-833: Deadlock |

## Vulnerability CVE-2022-4304

A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.9 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C |
| CWE | CWE-326: Inadequate Encryption Strength |

## Vulnerability CVE-2022-4450

The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the “name” (e.g. “CERTIFICATE"), any header data and the payload data. If the function succeeds then the “name_out”, “header” and “data” arguments are populated with pointers to buffers containing the relevant decoded data. The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internal uses of these functions are not vulnerable because the caller does not free the header argument if PEM_read_bio_ex() returns a failure code. These locations include the PEM_read_bio_TYPE() functions as well as the decoders introduced in OpenSSL 3.0. The OpenSSL asn1parse command line application is also impacted by this issue.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.9 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C |
| CWE | CWE-415: Double Free |

## Vulnerability CVE-2022-4662

A flaw incorrect access control in the Linux kernel USB core subsystem was found in the way user attaches usb device. A local user could use this flaw to crash the system.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-455: Non-exit on Failed Initialization |

### Vulnerability CVE-2022-20421

In binder_inc_ref_for_node of binder.c, there is a possible way to corrupt memory due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239630375References: Upstream kernel

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-20422

In emulation_proc_handler of armv8_deprecated.c, there is a possible way to corrupt memory due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-237540956References: Upstream kernel

| | |
|---|---|
| CVSS v3.1 Base Score | 7.0 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |

### Vulnerability CVE-2022-20566

In l2cap_chan_put of l2cap_core, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-165329981References: Upstream kernel

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-20572

In verity_target of dm-verity-target.c, there is a possible way to modify read-only files due to a missing permission check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-234475629References: Upstream kernel

| | |
|---|---|
| CVSS v3.1 Base Score | 6.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-863: Incorrect Authorization |

### Vulnerability CVE-2022-21123

Incomplete cleanup of multi-core shared buffers for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-459: Incomplete Cleanup |

### Vulnerability CVE-2022-21125

Incomplete cleanup of microarchitectural fill buffers on some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-459: Incomplete Cleanup |

### Vulnerability CVE-2022-21166

Incomplete cleanup in specific special register write operations for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-459: Incomplete Cleanup |

### Vulnerability CVE-2022-21505

A bug in the IMA subsystem was discovered which would incorrectly allow kexec to be used when kernel lockdown was enabled

| | |
|---|---|
| CVSS v3.1 Base Score | 6.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-305: Authentication Bypass by Primary Weakness |

### Vulnerability CVE-2022-26373

Non-transparent sharing of return predictor targets between contexts in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-311: Missing Encryption of Sensitive Data |

### Vulnerability CVE-2022-32250

net/netfilter/nf_tables_api.c in the Linux kernel through 5.18.1 allows a local user (able to create user/net namespaces) to escalate privileges to root because an incorrect NFT_STATEFUL_EXPR check leads to a use-after-free.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability 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.

| | |
|---|---|
| CVSS v3.1 Base Score | 3.3 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-203: Observable Discrepancy |

### Vulnerability CVE-2022-34918

An issue was discovered in the Linux kernel through 5.18.9. A type confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a local attacker to escalate privileges, a different vulnerability than CVE-2022-32250. (The attacker can obtain root access, but must start with an unprivileged user namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data in net/netfilter/nf_tables_api.c.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') |

### Vulnerability CVE-2022-36123

The Linux kernel before 5.18.13 lacks a certain clear operation for the block starting symbol (.bss). This allows Xen PV guest OS users to cause a denial of service or gain privileges.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-311: Missing Encryption of Sensitive Data |

### Vulnerability CVE-2022-36280

An out-of-bounds(OOB) memory access vulnerability was found in vmwgfx driver in drivers/gpu/vmxgfx/vmxgfx_kms.c in GPU component in the Linux kernel 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).

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2022-36879

An issue was discovered in the Linux kernel through 5.18.14. xfrm_expand_policies in net/xfrm/xfrm_policy.c can cause a refcount to be dropped twice.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2022-36946

nfqnl_mangle in net/netfilter/nfnetlink_queue.c in the Linux kernel through 5.18.14 allows remote attackers to cause a denial of service (panic) because, in the case of an nf_queue verdict with a one-byte nfta_payload attribute, an skb_pull can encounter a negative skb->len.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability 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.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |

### Vulnerability CVE-2022-39190

An issue was discovered in net/netfilter/nf_tables_api.c in the Linux kernel before 5.19.6. A denial of service can occur upon binding to an already bound chain.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-400: Uncontrolled Resource Consumption |

### Vulnerability 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.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-40768

drivers/scsi/stex.c in the Linux kernel through 5.19.9 allows local users to obtain sensitive information from kernel memory because stex_queuecommand_lck lacks a memset for the PASSTHRU_CMD case.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-668: Exposure of Resource to Wrong Sphere |

### Vulnerability CVE-2022-41218

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability 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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.0 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-41674

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 8.1 |
| CVSS Vector | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability 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.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.2 |
| CVSS Vector | CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |

### Vulnerability CVE-2022-41850

roccat_report_event in drivers/hid/hid-roccat.c in the Linux kernel through 5.19.12 has a race condition and resultant use-after-free in certain situations where a report is received while copying a report->value is in progress.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |

### Vulnerability CVE-2022-42328

Guests can trigger deadlock in Linux netback driver [This 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).

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-667: Improper Locking |

### Vulnerability CVE-2022-42329

Guests can trigger deadlock in Linux netback drive. 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).

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-667: Improper Locking |

### Vulnerability CVE-2022-42432

This vulnerability allows local attackers to disclose sensitive information on affected installations of the Linux Kernel 6.0-rc2. An attacker must first obtain the ability to execute high-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the nft_osf_eval function. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the kernel. Was ZDI-CAN-18540.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.4 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-457: Use of Uninitialized Variable |

### Vulnerability 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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-42719

A use-after-free in the mac80211 stack when parsing a multi-BSSID element in the Linux kernel 5.2 through 5.19.x before 5.19.16 could be used by attackers (able to inject WLAN frames) to crash the kernel and potentially execute code.

| | |
|---|---|
| CVSS v3.1 Base Score | 8.8 |
| CVSS Vector | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-42720

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-42721

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') |

### Vulnerability CVE-2022-42722

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2022-42895

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

| | |
|---|---|
| CVSS v3.1 Base Score | 6.5 |
| CVSS Vector | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-824: Access of Uninitialized Pointer |

### Vulnerability CVE-2022-42896

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://github.com/torvalds/linux/commit/711f8c3fb3db61897080468586b970c87c61d9e4

| | |
|---|---|
| CVSS v3.1 Base Score | 8.8 |
| CVSS Vector | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2022-43750

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2022-47518

An issue was discovered in the Linux kernel before 6.0.11. Missing validation of the number of channels in drivers/net/wireless/microchip/wilc1000/cfg80211.c in the WILC1000 wireless driver can trigger a heap-based buffer overflow when copying the list of operating channels from Wi-Fi management frames.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2022-47520

An issue was discovered in the Linux kernel before 6.0.11. Missing offset validation in drivers/net/wireless/microchip/wilc1000/hif.c in the WILC1000 wireless driver can trigger an out-of-bounds read when parsing a Robust Security Network (RSN) information element from a Netlink packet.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.1 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2022-47929

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2022-47946

An issue was discovered in the Linux kernel 5.10.x before 5.10.155. A use-after-free in io_sqpoll_wait_sq in fs/io_uring.c allows an attacker to crash the kernel, resulting in denial of service. finish_wait can be skipped. An attack can occur in some situations by forking a process and then quickly terminating it. NOTE: later kernel versions, such as the 5.15 longterm series, substantially changed the implementation of io_sqpoll_wait_sq.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-0215

The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.9 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-0286

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.4 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2023-0464

A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems.

Policy processing is disabled by default but can be enabled by passing the `-policy` argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()` function.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-295: Improper Certificate Validation |

### Vulnerability CVE-2023-0465

Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks.

Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether.

Policy processing is disabled by default but can be enabled by passing the `-policy` argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()` function.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C |
| CWE | CWE-295: Improper Certificate Validation |

### Vulnerability CVE-2023-0466

The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. However the implementation of the function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification.

As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy() function.

Instead the applications that require OpenSSL to perform certificate policy check need to use X509_VERIFY_PARAM_set1_policies() or explicitly enable the policy check by calling X509_VERIFY_PARAM_set_flags() with the X509_V_FLAG_POLICY_CHECK flag argument.

Certificate policy checks are disabled by default in OpenSSL and are not commonly used by applications.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C |
| CWE | CWE-295: Improper Certificate Validation |

### Vulnerability CVE-2023-0590

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-1077

In the Linux kernel, pick_next_rt_entity() may return a type confused entry, not detected by the BUG_ON condition, as the confused entry will not be NULL, but list_head.The buggy error condition would lead to a type confused entry with the list head,which would then be used as a type confused sched_rt_entity,causing memory corruption.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') |

### Vulnerability CVE-2023-1095

In nf_tables_updtable, if nf_tables_table_enable returns an error, nft_trans_destroy is called to free the transaction object. nft_trans_destroy() calls list_del(), but the transaction was never placed on a list – the list head is all zeroes, this results in a NULL pointer dereference.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2023-1206

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%.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.7 |
| CVSS Vector | CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-400: Uncontrolled Resource Consumption |

### Vulnerability CVE-2023-2898

There is a null-pointer-dereference flaw found in f2fs_write_end_io in fs/f2fs/data.c in the Linux kernel. This flaw allows a local privileged user to cause a denial of service problem.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2023-3141

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.1 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-3268

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.1 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2023-3338

A null pointer dereference flaw was found in the Linux kernel's DECnet networking protocol. This issue could allow a remote user to crash the system.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

## Vulnerability CVE-2023-3389

A use-after-free vulnerability in the Linux Kernel io_uring subsystem can be exploited to achieve local privilege escalation. Racing a io_uring cancel poll request with a linked timeout can cause a UAF in a hrtimer.

We recommend upgrading past commit ef7dfac51d8ed961b742218f526bd589f3900a59 (4716c73b188566865bdd79c3a6709696a224ac04 for 5.10 stable and 0e388fce7aec40992eadee654193cad345d62663 for 5.15 stable).

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

## Vulnerability CVE-2023-3446

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 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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C |
| CWE | CWE-1333: Inefficient Regular Expression Complexity |

## Vulnerability CVE-2023-3609

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

## Vulnerability CVE-2023-3610

A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation.

Flaw in the error handling of bound chains causes a use-after-free in the abort path of NFT_MSG_NEWRULE. The vulnerability requires CAP_NET_ADMIN to be triggered.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-3611

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2023-3772

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2023-3773

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 cause a 4 byte out-of-bounds read of XFRMA_MTIMER_THRESH when parsing netlink attributes, leading to potential leakage of sensitive heap data to userspace.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2023-3777

A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation.

When nf_tables_delrule() is flushing table rules, it is not checked whether the chain is bound and the chain's owner rule can also release the objects in certain circumstances.

We recommend upgrading past commit 6eaf41e87a223ae6f8e7a28d6e78384ad7e407f8.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-4004

A use-after-free flaw was found in the Linux kernel's netfilter in the way a user triggers the nft_pipapo_remove function with the element, without a NFT_SET_EXT_KEY_END. This issue could allow a local user to crash the system or potentially escalate their privileges on the system.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2023-4015

The netfilter subsystem in the Linux kernel did not properly handle bound chain deactivation in certain circumstances. A local attacker could possibly use this to cause a denial of service (system crash) or execute arbitrary code.

| | |
|---|---|
| CVSS v3.1 Base Score | 8.4 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2023-4273

This vulnerability exists in the implementation of the file name reconstruction function, which is responsible for reading file name entries from a directory index and merging file name parts belonging to one file into a single long file name. Since the file name characters are copied into a stack variable, a local privileged attacker could use this vulnerability to overflow the kernel stack.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.0 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C |
| CWE | CWE-121: Stack-based Buffer Overflow |

### Vulnerability CVE-2023-4623

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-4911

A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when launching binaries with SUID permission to execute code with elevated privileges.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-121: Stack-based Buffer Overflow |

### Vulnerability CVE-2023-4921

A use-after-free vulnerability in the Linux kernel's net/sched: sch_qfq component can be exploited to achieve local privilege escalation.

When the plug qdisc is used as a class of the qfq qdisc, sending network packets triggers use-after-free in qfq_dequeue() due to the incorrect .peek handler of sch_plug and lack of error checking in agg_dequeue().

We recommend upgrading past commit 8fc134fee27f2263988ae38920bc03da416b03d8.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-5178

A use-after-free vulnerability was found in drivers/nvme/target/tcp.cinnvmet_tcp_free_crypto‘ due to a logical bug in the NVMe-oF/TCP subsystem in the Linux kernel. This issue may allow a malicious local privileged user to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation problem.

| | |
|---|---|
| CVSS v3.1 Base Score | 8.8 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-5197

A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation.

Addition and removal of rules from chain bindings within the same transaction causes leads to use-after-free.

We recommend upgrading past commit f15f29fd4779be8a418b66e9d52979bb6d6c2325.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-5678

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C |
| CWE | CWE-754: Improper Check for Unusual or Exceptional Conditions |

### Vulnerability CVE-2023-5717

A heap out-of-bounds write vulnerability in the Linux kernel's Linux Kernel Performance Events (perf) component can be exploited to achieve local privilege escalation.

If perf_read_group() is called while an event's sibling_list is smaller than its child's sibling_list, it can increment or write to memory locations outside of the allocated buffer.

We recommend upgrading past commit 32671e3799ca2e4590773fd0e63aaa4229e50c06.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2023-6606

An out-of-bounds read vulnerability was found in smbCalcSize in fs/smb/client/netmisc.c in the Linux Kernel. This issue could allow a local attacker to crash the system or leak internal kernel information.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.1 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2023-6931

A heap out-of-bounds write vulnerability in the Linux kernel's Performance Events system component can be exploited to achieve local privilege escalation.

A perf_event's read_size can overflow, leading to an heap out-of-bounds increment or write in perf_read_group().

We recommend upgrading past commit 382c27f4ed28f803b1f1473ac2d8db0afc795a1b.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2023-6932

A use-after-free vulnerability in the Linux kernel's ipv4: igmp component can be exploited to achieve local privilege escalation.

A race condition can be exploited to cause a timer be mistakenly registered on a RCU read locked object which is freed by another thread.

We recommend upgrading past commit e2b706c691905fe78468c361aaabc719d0a496f1.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-7008

A vulnerability was found in systemd-resolved. This issue may allow systemd-resolved to accept records of DNSSEC-signed domains even when they have no signature, allowing man-in-the-middles (or the upstream DNS resolver) to manipulate records.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.9 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C |
| CWE | CWE-300: Channel Accessible by Non-Endpoint |

### Vulnerability CVE-2023-7104

A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classified as critical. This issue affects the function sessionReadRecord of the file ext/session/sqlite3session.c of the component make alltest Handler. The manipulation leads to heap-based buffer overflow. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-248999.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L |
| CWE | CWE-122: Heap-based Buffer Overflow |

### Vulnerability CVE-2023-23454

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).

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') |

### Vulnerability CVE-2023-23455

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).

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') |

### Vulnerability CVE-2023-23559

In rndis_query_oid in drivers/net/wireless/rndis_wlan.c in the Linux kernel through 6.1.5, there is an integer overflow in an addition.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-190: Integer Overflow or Wraparound |

### Vulnerability CVE-2023-26607

In the Linux kernel 6.0.8, there is an out-of-bounds read in ntfs_attr_find in fs/ntfs/attrib.c.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.1 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2023-31085

An issue was discovered in drivers/mtd/ubi/cdev.c in the Linux kernel 6.2. There is a divide-by-zero error in do_div(sz,mtd->erasesize), used indirectly by ctrl_cdev_ioctl, when mtd->erasesize is 0.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-369: Divide By Zero |

### Vulnerability CVE-2023-31436

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.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2023-32233

In the Linux kernel through 6.3.1, a use-after-free in Netfilter nf_tables when processing batch requests can be abused to perform arbitrary read and write operations on kernel memory. Unprivileged local users can obtain root privileges. This occurs because anonymous sets are mishandled.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2023-35001

Linux Kernel nftables Out-Of-Bounds Read/Write Vulnerability; nft_byteorder poorly handled vm register contents when CAP_NET_ADMIN is in any user or network namespace

| | |
|---|---|
| CVSS v3.1 Base Score | 7.8 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2023-35827

An issue was discovered in the Linux kernel through 6.3.8. A use-after-free was found in ravb_remove in drivers/net/ethernet/renesas/ravb_main.c.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.0 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2023-36660

The OCB feature in libnettle in Nettle 3.9 before 3.9.1 allows memory corruption.

| | |
|---|---|
| CVSS v3.1 Base Score | 9.8 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2023-37453

An issue was discovered in the USB subsystem in the Linux kernel through 6.4.2. There is an out-of-bounds and crash in read_descriptors in drivers/usb/core/sysfs.c.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.6 |
| CVSS Vector | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2023-39189

A flaw was found in the Netfilter subsystem in the Linux kernel. The nfnl_osf_add_callback function did not validate the user mode controlled opt_num field. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, leading to a crash or information disclosure.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.1 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:L/E:P/RL:O/RC:C |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2023-39192

A flaw was found in the Netfilter subsystem in the Linux kernel. The xt_u32 module did not validate the fields in the xt_u32 structure. This flaw allows a local privileged attacker to trigger an out-of-bounds read by setting the size fields with a value beyond the array boundaries, leading to a crash or information disclosure.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:L |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2023-39193

A flaw was found in the Netfilter subsystem in the Linux kernel. The sctp_mt_check did not validate the flag_count field. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, leading to a crash or information disclosure.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.1 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2023-39194

A flaw was found in the XFRM subsystem in the Linux kernel. The specific flaw exists within the processing of state filters, which can result in a read past the end of an allocated buffer. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, potentially leading to an information disclosure.

| | |
|---|---|
| CVSS v3.1 Base Score | 3.2 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2023-42753

An array indexing vulnerability was found in the netfilter subsystem of the Linux kernel. A missing macro could lead to a miscalculation of the `h->nets` array offset, providing attackers with the primitive to arbitrarily increment/decrement a memory buffer out-of-bound. This issue may allow a local user to crash the system or potentially escalate their privileges on the system.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.0 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2023-42754

A NULL pointer dereference flaw was found in the Linux kernel ipv4 stack. The socket buffer (skb) was assumed to be associated with a device before calling __ip_options_compile, which is not always the case if the skb is re-routed by ipvs. This issue may allow a local user with CAP_NET_ADMIN privileges to crash the system.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-476: NULL Pointer Dereference |

### Vulnerability CVE-2023-42755

A flaw was found in the IPv4 Resource Reservation Protocol (RSVP) classifier in the Linux kernel. The xprt pointer may go beyond the linear part of the skb, leading to an out-of-bounds read in the `rsvp_classify` function. This issue may allow a local user to crash the system and cause a denial of service.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H |
| CWE | CWE-125: Out-of-bounds Read |

### Vulnerability CVE-2023-45863

An issue was discovered in lib/kobject.c in the Linux kernel before 6.2.3. With root access, an attacker can trigger a race condition that results in a fill_kobj_path out-of-bounds write.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.4 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-787: Out-of-bounds Write |

### Vulnerability CVE-2023-45871

An issue was discovered in drivers/net/ethernet/intel/igb/igb_main.c in the IGB driver in the Linux kernel before 6.5.3. A buffer size may not be adequate for frames larger than the MTU.

| | |
|---|---|
| CVSS v3.1 Base Score | 9.8 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') |

### Vulnerability CVE-2023-48795

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 before1.3.9rc2), 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, 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; and there could be effects on Bitvise SSH through 9.31.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.9 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C |
| CVSS v4.0 Base Score | 8.2 |
| CVSS Vector | CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N |
| CWE | CWE-222: Truncation of Security-relevant Information |

### Vulnerability CVE-2023-50495

NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().

| | |
|---|---|
| CVSS v3.1 Base Score | 6.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2023-51384

In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2023-51385

In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C |
| CWE | CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |

### Vulnerability CVE-2023-51767

OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.0 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2024-0232

A heap use-after-free issue has been identified in SQLite in the jsonParseAddNodeArray() function in sqlite3.c. This flaw allows a local attacker to leverage a victim to pass specially crafted malicious input to the application, potentially causing a crash and leading to a denial of service.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.7 |
| CVSS Vector | CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2024-0553

A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from the response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. CVE-2024-0553 is designated as an incomplete resolution for CVE-2023-5981.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-203: Observable Discrepancy |

### Vulnerability CVE-2024-0567

A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTLS) rejects a certificate chain with distributed trust. This issue occurs when validating a certificate chain with cockpit-certificate-ensure. This flaw allows an unauthenticated, remote client or attacker to initiate a denial of service attack.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-347: Improper Verification of Cryptographic Signature |

### Vulnerability CVE-2024-0584

A use-after-free issue was found in igmp_start_timer in net/ipv4/igmp.c in the network sub-component in the Linux Kernel. This flaw allows a local user to observe a refcnt use-after-free issue when receiving an igmp query packet, leading to a kernel information leak.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N |
| CWE | CWE-416: Use After Free |

### Vulnerability CVE-2024-0684

A flaw was found in the GNU coreutils “split” program. A heap overflow with user-controlled data of multiple hundred bytes in length could occur in the line_bytes_split() function, potentially leading to an application crash and denial of service.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-122: Heap-based Buffer Overflow |

### Vulnerability CVE-2024-22365

linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked login process) via mkfifo because the openat call (for protect_dir) lacks O_DIRECTORY.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.5 |
| CVSS Vector | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-20: Improper Input Validation |

### Vulnerability CVE-2024-25062

An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. When using the XML Reader interface with DTD validation and XInclude expansion enabled, processing crafted XML documents can lead to an xmlValidatePopElement use-after-free.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.9 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-416: Use After Free |

## ADDITIONAL INFORMATION

This advisory is no longer maintained.
It listed vulnerabilities for firmware version V1.0 only; for V1.1 refer to Siemens Security Advisory SSA-265688 (https://cert-portal.siemens.com/productcert/html/ssa-265688.html).

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

## HISTORY DATA

| | |
|---|---|
| V1.0 (2023-06-13): | Publication Date |
| V1.1 (2023-07-11): | Added CVE-2022-4269, CVE-2023-3141, CVE-2023-3268, CVE-2023-31436, CVE-2023-32233 |
| V1.2 (2023-08-08): | Added CVE-2023-3446, CVE-2023-3389, CVE-2022-1015, CVE-2023-3609 |
| V1.3 (2023-09-12): | Added CVE-2023-3338 |
| V1.4 (2023-11-14): | Added CVE-2023-1206, CVE-2023-2898, CVE-2023-3610, CVE-2023-3611, CVE-2023-3772, CVE-2023-3773, CVE-2023-3777, CVE-2023-4004, CVE-2023-4015, CVE-2023-4273, CVE-2023-4623, CVE-2023-4921, CVE-2023-35001, CVE-2023-37453, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-42753, CVE-2023-42755 |
| V1.5 (2023-12-12): | Added CVE-2021-44879, CVE-2023-5178, CVE-2023-5197, CVE-2023-5678, CVE-2023-5717, CVE-2023-31085, CVE-2023-35827, CVE-2023-39189, CVE-2023-42754, CVE-2023-45863, CVE-2023-45871 |
| V1.6 (2024-01-09): | Added CVE-2023-48795 |
| V1.7 (2024-02-13): | Added CVE-2020-12762, CVE-2023-6606, CVE-2023-6931, CVE-2023-6932, CVE-2023-7008, CVE-2023-7104, CVE-2023-36660, CVE-2023-50495, CVE-2023-51384, CVE-2023-51385, CVE-2023-51767, CVE-2024-0232, CVE-2024-0553, CVE-2024-0567, CVE-2024-0584, CVE-2024-0684, CVE-2024-22365, CVE-2024-25062 |
| V1.8 (2024-04-09): | Added fix for SIMATIC S7-1500 TM MFP - GNU/Linux subsystem |

## TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.