

## **SSA-265688: Vulnerabilities in the additional GNU/Linux subsystem of the SIMATIC S7-1500 TM MFP V1.1**

Publication Date: 2024-04-09  
Last Update: 2025-10-14  
Current Version: V2.0  
CVSS v3.1 Base Score: 9.1  
CVSS v4.0 Base Score: 6.3

### **SUMMARY**

Multiple vulnerabilities have been identified in the additional GNU/Linux subsystem of the SIMATIC S7-1500 TM MFP V1.1.

Siemens is preparing fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

### **KNOWN AFFECTED PRODUCTS**

<b>Affected Product and Versions</b>	<b>Remediation</b>
SIMATIC S7-1500 TM MFP - GNU/Linux subsystem: All versions affected by <a href="#">all CVEs</a>	Currently no fix is available See recommendations from section <a href="#">Workarounds and Mitigations</a>

### **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

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-2021-4090**

An out-of-bounds (OOB) memory write flaw was found in the NFSD in the Linux kernel. Missing sanity may lead to a write beyond `bmval[bmlen-1]` in `nfsd4_decode_bitmap4` in `fs/nfsd/nfs4xdr.c`. In this flaw, a local attacker with user privilege may gain access to out-of-bounds memory, leading to a system integrity and confidentiality threat.

CVSS v3.1 Base Score	5.3
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-787: Out-of-bounds Write

### **Vulnerability CVE-2021-38202**

`fs/nfsd/trace.h` in the Linux kernel before 5.13.4 might allow remote attackers to cause a denial of service (out-of-bounds read in `strlen`) by sending NFS traffic when the trace event framework is being used for `nfsd`.

CVSS v3.1 Base Score	7.5
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-125: Out-of-bounds Read

### **Vulnerability CVE-2021-47002**

SUNRPC: null pointer dereference in `svc_rqst_free()`. When `alloc_pages_node()` returns null in `svc_rqst_alloc()`, the null `rq_scratch_page` pointer will be dereferenced when calling `put_page()` in `svc_rqst_free()`.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

### **Vulnerability CVE-2021-47107**

NFSD: READDIR buffer overflow. If a client sends a READDIR count argument that is too small (say, zero), then the buffer size calculation in the new `init_dirlist` helper functions results in an underflow, allowing the XDR stream functions to write beyond the actual buffer. This calculation has always been suspect. NFSD has never sanity-checked the READDIR count argument, but the old entry encoders managed the problem correctly. With the commits below, entry encoding changed, exposing the underflow to the pointer arithmetic in `xdr_reserve_space()`. Modern NFS clients attempt to retrieve as much data as possible for each READDIR request.

CVSS v3.1 Base Score	6.3
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L</a>
CWE	CWE-121: Stack-based Buffer Overflow

### **Vulnerability CVE-2021-47316**

`nfsd`: NULL dereference in `nfs3svc_encode_getaclres`.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

**Vulnerability CVE-2022-38096**

A NULL pointer dereference vulnerability was found in vmwgfx driver in drivers/gpu/vmxgfx/vmxgfx\_execbuf.c in GPU component of 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 6.3  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:H](#)  
CWE CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2022-43945**

The Linux kernel NFSD implementation prior to versions 5.19.17 and 6.0.2 are vulnerable to buffer overflow. NFSD tracks the number of pages held by each NFSD thread by combining the receive and send buffers of a remote procedure call (RPC) into a single array of pages. A client can force the send buffer to shrink by sending an RPC message over TCP with garbage data added at the end of the message. The RPC message with garbage data is still correctly formed according to the specification and is passed forward to handlers. Vulnerable code in NFSD is not expecting the oversized request and writes beyond the allocated buffer space.

CVSS 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](#)  
CWE CWE-131: Incorrect Calculation of Buffer Size

**Vulnerability CVE-2022-48827**

NFSD: vulnerability caused by loff\_t overflow on the server when a client reads near the maximum offset, causing the server to return an EINVAL error, which the client retries indefinitely, instead of handling out-of-range READ requests by returning a short result with an EOF flag.

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

**Vulnerability CVE-2022-48828**

NFSD: Vulnerability caused by an underflow in ia\_size due to a mismatch between signed and unsigned 64-bit file size values, which can cause issues when handling large file sizes from NFS clients.

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-20: Improper Input Validation

**Vulnerability CVE-2022-48829**

NFSD: Vulnerability handling large file sizes for NFSv3 improperly capping client size values larger than s64\_max, leading to unexpected behavior and potential data corruption.

CVSS v3.1 Base Score 7.1  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H](#)  
CWE CWE-253: Incorrect Check of Function Return Value

**Vulnerability CVE-2023-1652**

A use-after-free flaw was found in nfsd4\_ssc\_setup\_dul in fs/nfsd/nfs4proc.c in the NFS filesystem in the Linux Kernel. This issue could allow a local attacker to crash the system or it may lead to a kernel information leak problem.

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](#)  
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	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L</a>
CWE	CWE-606: Unchecked Input for Loop Condition

### **Vulnerability CVE-2023-6121**

An out-of-bounds read vulnerability was found in the NVMe-oF/TCP subsystem in the Linux kernel. This issue may allow a remote attacker to send a crafted TCP packet, triggering a heap-based buffer overflow that results in `kmalloc` data being printed and potentially leaked to the kernel ring buffer (`dmesg`).

CVSS v3.1 Base Score	4.3
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N</a>
CWE	CWE-125: Out-of-bounds Read

### **Vulnerability CVE-2023-6129**

The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions.

If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences.

The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions.

The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service.

The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used. This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue.

CVSS v3.1 Base Score	6.5
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H</a>
CWE	CWE-787: Out-of-bounds Write

### **Vulnerability CVE-2023-6237**

Checking excessively long invalid RSA public keys may take a long time. Applications that use the function `EVP_PKEY_public_check()` to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function `EVP_PKEY_public_check()` is called on RSA public keys, a computation is done to confirm that the RSA modulus, `n`, is composite. For valid RSA keys, `n` is a product of two or more large primes and this computation completes quickly. However, if `n` is an overly large prime, then this computation would take a long time. An application that calls `EVP_PKEY_public_check()` and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function `EVP_PKEY_public_check()` is not called from other OpenSSL functions however it is called from the OpenSSL `pkey` command line application. For that reason that application is also vulnerable if used with the `-pubin` and `-check` options on untrusted data. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue.

CVSS v3.1 Base Score	5.9
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-400: Uncontrolled Resource Consumption

### **Vulnerability CVE-2023-6817**

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

The function nft\_pipapo\_walk did not skip inactive elements during set walk which could lead double deactivations of PIPAPO (Pile Packet Policies) elements, leading to use-after-free.

We recommend upgrading past commit 317eb9685095678f2c9f5a8189de698c5354316a.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

### **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	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
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	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2023-28746**

Information exposure through microarchitectural state after transient execution from some register files for some Intel(R) Atom(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.

CVSS v3.1 Base Score	6.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N</a>
CWE	CWE-1342: Information Exposure through Microarchitectural State after Transient Execution

### **Vulnerability CVE-2023-45898**

The Linux kernel before 6.5.4 has an es1 use-after-free in fs/ext4/extents\_status.c, related to ext4\_es\_insert\_extent.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-20: Improper Input Validation

**Vulnerability CVE-2023-47233**

The brcm80211 component in the Linux kernel through 6.5.10 has a brcmf\_cfg80211\_detach use-after-free in the device unplugging (disconnect the USB by hotplug) code. For physically proximate attackers with local access, this “could be exploited in a real world scenario.” This is related to brcmf\_cfg80211\_escan\_timeout\_worker in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c.

CVSS v3.1 Base Score 4.3  
CVSS Vector [CVSS:3.1/AV:P/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H](#)  
CWE CWE-416: Use After Free

**Vulnerability CVE-2023-50781**

A flaw was found in m2crypto. This issue may allow a remote attacker to decrypt captured messages in TLS servers that use RSA key exchanges, which may lead to exposure of confidential or sensitive data.

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](#)  
CWE CWE-327: Use of a Broken or Risky Cryptographic Algorithm

**Vulnerability CVE-2023-52447**

bpf: Defer the free of inner map when necessary when updating or deleting an inner map in map array or map htab, the map may still be accessed by non-sleepable program or sleepable program. However bpf\_map\_fd\_put\_ptr() decreases the ref-counter of the inner map directly through bpf\_map\_put(), if the ref-counter is the last one (which is true for most cases), the inner map will be freed by ops->map\_free() in a kworker. But for now, most .map\_free() callbacks don't use synchronize\_rcu() or its variants to wait for the elapse of a RCU grace period, so after the invocation of ops->map\_free completes, the bpf program which is accessing the inner map may incur use-after-free vulnerability.

CVSS v3.1 Base Score 3.9  
CVSS Vector [CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:L](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2023-52458**

In the Linux kernel, the following vulnerability has been resolved:

block: add check that partition length needs to be aligned with block size

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-2023-52614**

In the Linux kernel, the following vulnerability has been resolved:

PM / devfreq: Fix buffer overflow in trans\_stat\_show

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-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

**Vulnerability CVE-2023-52620**

In the Linux kernel, the following vulnerability has been resolved:

netfilter: nf\_tables: disallow timeout for anonymous sets

Never used from userspace, disallow these parameters.

CVSS v3.1 Base Score	2.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L</a>
CWE	CWE-99: Improper Control of Resource Identifiers ('Resource Injection')

**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	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N</a>
CWE	CWE-416: Use After Free

**Vulnerability CVE-2024-0727**

Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack. Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: `PKCS12_parse()`, `PKCS12_unpack_p7data()`, `PKCS12_unpack_p7encdata()`, `PKCS12_unpack_authsafes()` and `PKCS12_newpass()`. We have also fixed a similar issue in `SMIME_write_PKCS7()`. However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-2511**

Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions. An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service. This problem can occur in TLSv1.3 if the non-default `SSL_OP_NO_TICKET` option is being used (but not if `early_data` support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

CVSS v3.1 Base Score	3.7
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L</a>
CWE	CWE-400: Uncontrolled Resource Consumption

**Vulnerability CVE-2024-5535**

Issue summary: Calling the OpenSSL API function `SSL_select_next_proto` with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application behaviour or a crash. In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the `SSL_select_next_proto` function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function `SSL_select_next_proto` is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The `SSL_select_next_proto` function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where `SSL_select_next_proto` is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the `SSL_select_next_proto` function has been called as expected (with the list supplied by the client passed in the `client/client_len` parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the `client/client_len` parameters, and has additionally failed to correctly handle a “no overlap” response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the `SSL_select_next_proto` function is accidentally called with a `client_len` of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available.

CVSS v3.1 Base Score	5.9
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N</a>
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

**Vulnerability CVE-2024-9143**

Issue summary: Use of the low-level GF(2m) elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes. Impact summary: Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only "named curves" are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary (GF(2m)) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low. In particular, the X9.62 encoding is used for ECC keys in X.509 certificates, so problematic inputs cannot occur in the context of processing X.509 certificates. Any problematic use-cases would have to be using an "exotic" curve encoding. The affected APIs include: EC\_GROUP\_new\_curve\_GF2m(), EC\_GROUP\_new\_from\_params(), and various supporting BN\_GF2m\_\*() functions. Applications working with "exotic" explicit binary (GF(2m)) curve parameters, that make it possible to represent invalid field polynomials with a zero constant term, via the above or similar APIs, may terminate abruptly as a result of reading or writing outside of array bounds. Remote code execution cannot easily be ruled out. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.

CVSS v3.1 Base Score	4.3
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N</a>
CVSS v4.0 Base Score	6.3
CVSS Vector	<a href="#">CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N</a>
CWE	CWE-787: Out-of-bounds Write

**Vulnerability CVE-2024-22099**

NULL Pointer Dereference vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (net, bluetooth modules) allows Overflow Buffers. This vulnerability is associated with program files /net/bluetooth/rfcomm/core.C.

This issue affects Linux kernel: v2.6.12-rc2.

CVSS v3.1 Base Score	6.3
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-23307**

Integer Overflow or Wraparound vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (md, raid, raid5 modules) allows Forced Integer Overflow.

CVSS v3.1 Base Score	4.4
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-190: Integer Overflow or Wraparound

**Vulnerability CVE-2024-23848**

In the Linux kernel through 6.7.1, there is a use-after-free in cec\_queue\_msg\_fh, related to drivers/media/cec/core/cec-adap.c and drivers/media/cec/core/cec-api.c.

CVSS v3.1 Base Score	7.5
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2024-24857**

A race condition was found in the Linux kernel's net/bluetooth device driver in `conn_info_min,max_age_set()` function. This can result in integrity overflow issue, possibly leading to bluetooth connection abnormality or denial of service.

CVSS v3.1 Base Score 4.6  
CVSS Vector [CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:L](#)  
CWE CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-24858**

A race condition was found in the Linux kernel's net/bluetooth in `conn,adv_min,max_interval_set()` function. This can result in l2cap connection or broadcast abnormality issue, possibly leading to denial of service.

CVSS v3.1 Base Score 4.6  
CVSS Vector [CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:H](#)  
CWE CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-24859**

A race condition was found in the Linux kernel's net/bluetooth in `sniff_min,max_interval_set()` function. This can result in a bluetooth sniffing exception issue, possibly leading denial of service.

CVSS v3.1 Base Score 4.6  
CVSS Vector [CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:H](#)  
CWE CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-25739**

`create_empty_lvol` in `drivers/mtd/ubi/vtbl.c` in the Linux kernel through 6.7.4 can attempt to allocate zero bytes, and crash, because of a missing check for `ubi->leb_size`.

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-754: Improper Check for Unusual or Exceptional Conditions

### **Vulnerability CVE-2024-26629**

`nfsd`: The test on `so_count` in `nfsd4_release_lockowner()` is potentially harmful. It can transiently return a false positive resulting in a return of `NFS4ERR_LOCKS_HELD` when in fact no locks are held. This is clearly a protocol violation and with the Linux NFS client it can cause incorrect behaviour.

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-393: Return of Wrong Status Code

### **Vulnerability CVE-2024-26642**

In the Linux kernel, the following vulnerability has been resolved:

netfilter: `nf_tables`: disallow anonymous set with timeout flag

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-20: Improper Input Validation

### **Vulnerability CVE-2024-26643**

In the Linux kernel, the following vulnerability has been resolved:

netfilter: nf\_tables: mark set as dead when unbinding anonymous set with timeout

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-667: Improper Locking

### **Vulnerability CVE-2024-26651**

sr9800: Local Denial of Service Vulnerability.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26659**

xhci: isoc Babble and Buffer Overrun events are not handled properly.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26787**

mmc: mmci: stm32: Fixed issue with overlapping mappings in the DMA API.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26810**

In the Linux kernel, the following vulnerability has been resolved:

vfio/pci: Lock external INTx masking ops

CVSS v3.1 Base Score	4.4
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-26812**

In the Linux kernel, the following vulnerability has been resolved:

vfio/pci: Create persistent INTx handler

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

### **Vulnerability CVE-2024-26816**

x86, relocs: relocations in .notes section. When building with CONFIG\_XEN\_PV=y, .text symbols are emitted into the .notes section so that Xen can find the "startup\_xen" entry point.

CVSS v3.1 Base Score	6.0
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:H</a>
CWE	CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer

### **Vulnerability CVE-2024-26820**

hv\_netvsc: Register VF in netvsc\_probe if NET\_DEVICE\_REGISTER missed.

CVSS v3.1 Base Score	4.4
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-99: Improper Control of Resource Identifiers ('Resource Injection')

### **Vulnerability CVE-2024-26851**

netfilter: nf\_contrack\_h323: Add protection for bmp length out of range.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26852**

net/ipv6: possible UAF in ip6\_route\_mpath\_notify().

CVSS v3.1 Base Score	7.0
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26855**

net: ice: Fix potential NULL pointer dereference in ice\_bridge\_setlink().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26859**

net/bnx2x: Race condition leading to system crash during EEH error handling.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26861**

wireguard: receive: data-race around receiving\_counter.counter.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26863**

In the Linux kernel, the following vulnerability has been resolved: hsr: Fix uninit-value access in hsr\_get\_node().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-908: Use of Uninitialized Resource

**Vulnerability CVE-2024-26870**

NFSv4.2: fix nfs4\_listxattr kernel BUG at mm/usercopy.c:102.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

**Vulnerability CVE-2024-26872**

RDMA/srpt: use-after-free Write in srpt\_refresh\_port().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

**Vulnerability CVE-2024-26875**

media: pvrusb2: fix uaf in pvr2\_context\_set\_notify.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

**Vulnerability CVE-2024-26877**

crypto: xilinx - call finalize with bh disabled.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

**Vulnerability CVE-2024-26878**

In the Linux kernel, the following vulnerability has been resolved: quota: Fix potential NULL pointer dereference.

CVSS v3.1 Base Score	4.7
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-26880**

In the Linux kernel, the following vulnerability has been resolved: dm: call the resume method on internal suspend.

CVSS v3.1 Base Score	4.4
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-99: Improper Control of Resource Identifiers ('Resource Injection')

**Vulnerability CVE-2024-26882**

net: ip\_tunnel: make sure to pull inner header in ip\_tunnel\_rcv().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26883**

bpf: Fix stackmap overflow check on 32-bit arches.

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-20: Improper Input Validation

### **Vulnerability CVE-2024-26884**

bpf: Fix hashtable overflow check on 32-bit arches.

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-20: Improper Input Validation

### **Vulnerability CVE-2024-26885**

In the Linux kernel, the following vulnerability has been resolved:

bpf: Fix DEVMAP\_HASH overflow check on 32-bit arches

The devmap code allocates a number hash buckets equal to the next power of two of the max\_entries value provided when creating the map. When rounding up to the next power of two, the 32-bit variable storing the number of buckets can overflow, and the code checks for overflow by checking if the truncated 32-bit value is equal to 0. However, on 32-bit arches the rounding up itself can overflow mid-way through, because it ends up doing a left-shift of 32 bits on an unsigned long value. If the size of an unsigned long is four bytes, this is undefined behaviour, so there is no guarantee that we'll end up with a nice and tidy 0-value at the end.

Syzbot managed to turn this into a crash on arm32 by creating a DEVMAP\_HASH with max\_entries > 0x80000000 and then trying to update it. Fix this by moving the overflow check to before the rounding up operation.

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

### **Vulnerability CVE-2024-26889**

Bluetooth: hci\_core: Fix possible buffer overflow.

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-20: Improper Input Validation

### **Vulnerability CVE-2024-26891**

iommu/vt-d: Don't issue ATS Invalidation request when device is disconnected.

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-20: Improper Input Validation

### **Vulnerability CVE-2024-26894**

ACPI: processor\_idle: Fix memory leak in acpi\_processor\_power\_exit().

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-20: Improper Input Validation

### **Vulnerability CVE-2024-26895**

wifi: wilc1000: prevent use-after-free on vif when cleaning up all interfaces.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26897**

wifi: ath9k: delay all of ath9k\_wmi\_event\_tasklet() until init is complete.

CVSS v3.1 Base Score	4.7
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26898**

In the Linux kernel, the following vulnerability has been resolved: aoe: fix the potential use-after-free problem in aoecmd\_cfg\_pkts.

CVSS v3.1 Base Score	7.0
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2024-26901**

In the Linux kernel, the following vulnerability has been resolved: do\_sys\_name\_to\_handle(): use kzalloc() to fix kernel-infoleak.

CVSS v3.1 Base Score	5.3
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L</a>
CWE	CWE-908: Use of Uninitialized Resource

### **Vulnerability CVE-2024-26903**

Bluetooth: rfcomm: Fixed null-ptr-deref in rfcomm\_check\_security.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26906**

x86/mm: Disallow vsyscall page read for copy\_from\_kernel\_nofault().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26907**

RDMA/mlx5: Fixed fortify source warning while accessing Eth segment.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-26920**

In the Linux kernel, the following vulnerability has been resolved:

tracing/trigger: Fix to return error if failed to alloc snapshot

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-908: Use of Uninitialized Resource

### **Vulnerability CVE-2024-26923**

In the Linux kernel, the following vulnerability has been resolved: af\_unix: Fix garbage collector racing against connect().

CVSS v3.1 Base Score	7.0
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-26925**

In the Linux kernel, the following vulnerability has been resolved: netfilter: nf\_tables: release mutex after nft\_gc\_seq\_end from abort path The commit mutex should not be released during the critical section between nft\_gc\_seq\_begin() and nft\_gc\_seq\_end(), otherwise, async GC worker could collect expired objects and get the released commit lock within the same GC sequence. nf\_tables\_module\_autoload() temporarily releases the mutex to load module dependencies, then it goes back to replay the transaction again. Move it at the end of the abort phase after nft\_gc\_seq\_end() is called.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-667: Improper Locking

### **Vulnerability CVE-2024-26934**

In the Linux kernel, the following vulnerability has been resolved:

USB: core: Fix deadlock in usb\_deauthorize\_interface()

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-667: Improper Locking

### **Vulnerability CVE-2024-26935**

In the Linux kernel, the following vulnerability has been resolved:

scsi: core: Fix unremoved procs host directory regression

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

### **Vulnerability CVE-2024-26937**

In the Linux kernel, the following vulnerability has been resolved:

drm/i915/gt: Reset queue\_priority\_hint on parking

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-617: Reachable Assertion

### **Vulnerability CVE-2024-26950**

In the Linux kernel, the following vulnerability has been resolved:

wireguard: netlink: access device through ctx instead of peer

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

### **Vulnerability CVE-2024-26951**

In the Linux kernel, the following vulnerability has been resolved:

wireguard: netlink: check for dangling peer via is\_dead instead of empty list

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2024-26958**

In the Linux kernel, the following vulnerability has been resolved:

nfs: fix UAF in direct writes

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2024-26960**

In the Linux kernel, the following vulnerability has been resolved:

mm: swap: fix race between free\_swap\_and\_cache() and swapoff()

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-26961**

In the Linux kernel, the following vulnerability has been resolved:

mac802154: fix llsec key resources release in mac802154\_llsec\_key\_del

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2024-26973**

In the Linux kernel, the following vulnerability has been resolved: fat: fix uninitialized field in nostale filehandles When fat\_encode\_fh\_nostale() encodes file handle without a parent it stores only first 10 bytes of the file handle. However the length of the file handle must be a multiple of 4 so the file handle is actually 12 bytes long and the last two bytes remain uninitialized. This is not great as we potentially leak uninitialized information with the handle to userspace. Properly initialize the full handle length.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-457: Use of Uninitialized Variable

### **Vulnerability CVE-2024-26974**

In the Linux kernel, the following vulnerability has been resolved:

crypto: qat - resolve race condition during AER recovery

CVSS v3.1 Base Score	7.0
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

### **Vulnerability CVE-2024-26982**

In the Linux kernel, the following vulnerability has been resolved: Squashfs: check the inode number is not the invalid value of zero

CVSS v3.1 Base Score	7.1
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H</a>
CWE	CWE-125: Out-of-bounds Read

### **Vulnerability CVE-2024-26988**

In the Linux kernel, the following vulnerability has been resolved:

init/main.c: Fix potential static\_command\_line memory overflow

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

### **Vulnerability CVE-2024-26993**

In the Linux kernel, the following vulnerability has been resolved:

fs: sysfs: Fix reference leak in sysfs\_break\_active\_protection()

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-27004**

In the Linux kernel, the following vulnerability has been resolved:

clk: Get runtime PM before walking tree during disable\_unused

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-667: Improper Locking

### **Vulnerability CVE-2024-27013**

In the Linux kernel, the following vulnerability has been resolved:

tun: limit printing rate when illegal packet received by tun dev

vhost\_worker will call tun call backs to receive packets. If too many illegal packets arrives, tun\_do\_read will keep dumping packet contents. When console is enabled, it will costs much more cpu time to dump packet and soft lockup will be detected.

net\_ratelimit mechanism can be used to limit the dumping rate.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

**Vulnerability CVE-2024-27020**

In the Linux kernel, the following vulnerability has been resolved: netfilter: nf\_tables: Fix potential data-race in nft\_expr\_type\_get().

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-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

**Vulnerability CVE-2024-27024**

Vulnerability in the Linux kernel: net/rds: WARNING in rds\_conn\_connect\_if\_down If connection isn't established yet, get\_mr() will fail, trigger connection after get\_mr().

CVSS v3.1 Base Score 8.8  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-27025**

Vulnerability in Linux kernel: nbd: null check for nla\_nest\_start nla\_nest\_start() may fail and return NULL. Insert a check and set errno based on other call sites within the same source code.

CVSS v3.1 Base Score 8.8  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-27038**

Vulnerability in Linux kernel: clk: clk\_core\_get NULL dereference It is possible for clk\_core\_get to dereference a NULL in the following sequence: clk\_core\_get() of clk\_get\_hw\_from\_clk\_spec() \_\_of\_clk\_get\_hw\_from\_provider() \_\_clk\_get\_hw() \_\_clk\_get\_hw() can return NULL which is dereferenced by clk\_core\_get() at hw->core. Prior to commit dde4eff47c82 ("clk: Look for parents with clkdev based clk\_lookups") the check IS\_ERR\_OR\_NULL() was performed which would have caught the NULL. Reading the description of this function it talks about returning NULL but that cannot be so at the moment. Update the function to check for hw before dereferencing it and return NULL if hw is NULL.

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](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-27047**

Vulnerability in Linux kernel: net: phy: phy\_get\_internal\_delay accessing an empty array The phy\_get\_internal\_delay function could try to access to an empty array in the case that the driver is calling phy\_get\_internal\_delay without defining delay\_values and rx-internal-delay-ps or tx-internal-delay-ps is defined to 0 in the device-tree. This will lead to "unable to handle kernel NULL pointer dereference at virtual address 0".

CVSS v3.1 Base Score 6.2  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-27052**

Vulnerability in Linux kernel: wifi: rtl8xxxu: add cancel\_work\_sync() for c2hcmd\_work The workqueue might still be running, when the driver is stopped.

CVSS v3.1 Base Score 8.8  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)  
CWE CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-27053**

Vulnerability in the Linux kernel: wifi: wilc1000: RCU usage in connect path

CVSS v3.1 Base Score 9.1  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H](#)  
CWE CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-27059**

In the Linux kernel, the following vulnerability has been resolved:

USB: usb-storage: Prevent divide-by-0 error in isd200\_ata\_command

The isd200 sub-driver in usb-storage uses the HEADS and SECTORS values in the ATA ID information to calculate cylinder and head values when creating a CDB for READ or WRITE commands. The calculation involves division and modulus operations, which will cause a crash if either of these values is 0. While this never happens with a genuine device, it could happen with a flawed or subversive emulation, as reported by the syzbot fuzzer.

Protect against this possibility by refusing to bind to the device if either the ATA\_ID\_HEADS or ATA\_ID\_SECTORS value in the device's ID information is 0. This requires isd200\_Initialization() to return a negative error code when initialization fails; currently it always returns 0 (even when there is an error).

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-369: Divide By Zero

### **Vulnerability CVE-2024-27065**

In the Linux kernel, the following vulnerability has been resolved: netfilter: nf\_tables: do not compare internal table flags on updates Restore skipping transaction if table update does not modify flags.

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](#)  
CWE CWE-1287: Improper Validation of Specified Type of Input

### **Vulnerability CVE-2024-27072**

In the Linux kernel, the following vulnerability has been resolved:

media: usbtv: Remove useless locks in usbtv\_video\_free()

Remove locks calls in usbtv\_video\_free() because are useless and may led to a deadlock as reported here: <https://syzkaller.appspot.com/x/bisect.txt?x=166dc872180000> Also remove usbtv\_stop() call since it will be called when unregistering the device.

Before 'c838530d230b' this issue would only be noticed if you disconnect while streaming and now it is noticeable even when disconnecting while not streaming.

[hverkuil: fix minor spelling mistake in log message]

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-667: Improper Locking

### **Vulnerability CVE-2024-27076**

Vulnerability in the Linux kernel: media: imx: csc/scaler: v4l2\_ctrl\_handler memory leak Free the memory allocated in v4l2\_ctrl\_handler\_init on release.

CVSS v3.1 Base Score 8.8  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)  
CWE CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-27077**

Vulnerability in Linux kernel: media: v4l2-mem2mem: a memleak in v4l2\_m2m\_register\_entity The entity->name (i.e. name) is allocated in v4l2\_m2m\_register\_entity but isn't freed in its following error-handling paths. This patch adds such deallocation to prevent memleak of entity->name.

CVSS v3.1 Base Score 8.8  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)  
CWE CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-27078**

Vulnerability in Linux kernel: media: v4l2-tpg: some memleaks in tpg\_alloc In tpg\_alloc, resources should be deallocated in each and every error-handling paths, since they are allocated in for statements. Otherwise there would be memleaks because tpg\_free is called only when tpg\_alloc return 0.

CVSS v3.1 Base Score 8.8  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)  
CWE CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-27395**

In the Linux kernel, the following vulnerability has been resolved:

net: openvswitch: Fix Use-After-Free in ovs\_ct\_exit

Since kfree\_rcu, which is called in the hlist\_for\_each\_entry\_rcu traversal of ovs\_ct\_limit\_exit, is not part of the RCU read critical section, it is possible that the RCU grace period will pass during the traversal and the key will be free.

To prevent this, it should be changed to hlist\_for\_each\_entry\_safe.

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-2024-27396**

In the Linux kernel, the following vulnerability has been resolved:

net: gtp: Fix Use-After-Free in gtp\_dellink

Since call\_rcu, which is called in the hlist\_for\_each\_entry\_rcu traversal of gtp\_dellink, is not part of the RCU read critical section, it is possible that the RCU grace period will pass during the traversal and the key will be free.

To prevent this, it should be changed to hlist\_for\_each\_entry\_safe.

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-2024-27397**

In the Linux kernel, the following vulnerability has been resolved:

netfilter: nf\_tables: use timestamp to check for set element timeout

Add a timestamp field at the beginning of the transaction, store it in the nftables per-netns area.

Update set backend .insert, .deactivate and sync gc path to use the timestamp, this avoids that an element expires while control plane transaction is still unfinished.

.lookup and .update, which are used from packet path, still use the current time to check if the element has expired. And .get path and dump also since this runs lockless under rcu read size lock. Then, there is async gc which also needs to check the current time since it runs asynchronously from a workqueue.

CVSS v3.1 Base Score	7.0
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2024-27419**

In the Linux kernel, the following vulnerability has been resolved: netrom: data-races around sysctl\_net\_busy\_read We need to protect the reader reading the sysctl value because the value can be changed concurrently.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-27431**

In the Linux kernel, the following vulnerability has been resolved: cpumap: Zero-initialise xdp\_rxq\_info struct before running XDP program When running an XDP program that is attached to a cpumap entry, we don't initialise the xdp\_rxq\_info data structure being used in the xdp\_buff that backs the XDP program invocation. Tobias noticed that this leads to random values being returned as the xdp\_md->rx\_queue\_index value for XDP programs running in a cpumap. This means we're basically returning the contents of the uninitialised memory, which is bad. Fix this by zero-initialising the rxq data structure before running the XDP program.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-27436**

In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: Stop parsing channels bits when all channels are found. If a usb audio device sets more bits than the amount of channels it could write outside of the map array.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-27437**

In the Linux kernel, the following vulnerability has been resolved:

vfio/pci: Disable auto-enable of exclusive INTx IRQ

Currently for devices requiring masking at the irqchip for INTx, ie. devices without DisINTx support, the IRQ is enabled in request\_irq() and subsequently disabled as necessary to align with the masked status flag. This presents a window where the interrupt could fire between these events, resulting in the IRQ incrementing the disable depth twice. This would be unrecoverable for a user since the masked flag prevents nested enables through vfio.

Instead, invert the logic using IRQF\_NO\_AUTOEN such that exclusive INTx is never auto-enabled, then unmask as required.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-33621**

In the Linux kernel, the following vulnerability has been resolved: ipvlan: Dont Use skb->sk in ipvlan\_process\_v4 / 6\_outbound.

CVSS v3.1 Base Score	4.4
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-1287: Improper Validation of Specified Type of Input

### **Vulnerability CVE-2024-33847**

f2fs: compress: Released compress inode f2fs image may be corrupted. The reason is partial truncation assume compressed inode has reserved blocks, after partial truncation, valid block count may change w/o .i\_blocks and .total\_valid\_block\_count update, resulting in corruption.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-34027**

f2fs: compress: filesystem metadata including blkaddr in dnode, inode fields and .total\_valid\_block\_count may be corrupted after SPO case.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-35789**

In the Linux kernel, the following vulnerability has been resolved:

wifi: mac80211: check/clear fast rx for non-4addr sta VLAN changes

When moving a station out of a VLAN and deleting the VLAN afterwards, the fast\_rx entry still holds a pointer to the VLAN's netdev, which can cause use-after-free bugs. Fix this by immediately calling ieee80211\_check\_fast\_rx after the VLAN change.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-400: Uncontrolled Resource Consumption

### **Vulnerability CVE-2024-35805**

In the Linux kernel, the following vulnerability has been resolved:

dm snapshot: fix lockup in dm\_exception\_table\_exit

There was reported lockup when we exit a snapshot with many exceptions. Fix this by adding "cond\_resched" to the loop that frees the exceptions.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-667: Improper Locking

### **Vulnerability CVE-2024-35807**

In the Linux kernel, the following vulnerability has been resolved: ext4: fix corruption during on-line resize.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-400: Uncontrolled Resource Consumption

### **Vulnerability CVE-2024-35811**

In the Linux kernel, the following vulnerability has been resolved:

wifi: brcmfmac: Fix use-after-free bug in brcmf\_cfg80211\_detach

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2024-35813**

In the Linux kernel, the following vulnerability has been resolved:

mmc: core: Avoid negative index with array access

Commit 4d0c8d0aef63 ("mmc: core: Use mrq.sbc in close-ended ffu") assigns prev\_idata = idatas[i - 1], but doesn't check that the iterator i is greater than zero. Let's fix this by adding a check.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-129: Improper Validation of Array Index

### **Vulnerability CVE-2024-35815**

In the Linux kernel, the following vulnerability has been resolved:

fs/aio: Check IOCB\_AIO\_RW before the struct aio\_kiocrb conversion

The first kiocrb\_set\_cancel\_fn() argument may point at a struct kiocrb that is not embedded inside struct aio\_kiocrb. With the current code, depending on the compiler, the req->ki\_ctx read happens either before the IOCB\_AIO\_RW test or after that test. Move the req->ki\_ctx read such that it is guaranteed that the IOCB\_AIO\_RW test happens first.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-237: Improper Handling of Structural Elements

### **Vulnerability CVE-2024-35823**

In the Linux kernel, the following vulnerability has been resolved:

vt: fix unicode buffer corruption when deleting characters

This is the same issue that was fixed for the VGA text buffer in commit 39cdb68c64d8 ("vt: fix memory overlapping when deleting chars in the buffer"). The cure is also the same i.e. replace memcpy() with memmove() due to the overlapping buffers.

CVSS v3.1 Base Score	5.3
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L</a>
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

### **Vulnerability CVE-2024-35828**

In the Linux kernel, the following vulnerability has been resolved: wifi: libertas: some memleaks in lbs\_allocate\_cmd\_buffer() In the for statement of lbs\_allocate\_cmd\_buffer(), if the allocation of cmdarray[i].cmdbuf fails, both cmdarray and cmdarray[i].cmdbuf needs to be freed. Otherwise, there will be memleaks in lbs\_allocate\_cmd\_buffer().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-35845**

wifi: iwlmwifi: dbg-tlv: ensure NUL termination The iwlmfw\_ini\_debug\_info\_tlv is used as a string, so we must ensure the string is terminated correctly before using it.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-35849**

In the Linux kernel, the following vulnerability has been resolved:

btrfs: fix information leak in btrfs\_ioctl\_logical\_to\_ino()

CVSS v3.1 Base Score	7.1
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H</a>
CWE	CWE-908: Use of Uninitialized Resource

### **Vulnerability CVE-2024-35877**

In the Linux kernel, the following vulnerability has been resolved:

x86/mm/pat: fix VM\_PAT handling in COW mappings

PAT handling won't do the right thing in COW mappings: the first PTE (or, in fact, all PTEs) can be replaced during write faults to point at anon folios. Reliably recovering the correct PFN and cachemode using `follow_phys()` from PTEs will not work in COW mappings.

Using `follow_phys()`, we might just get the address+protection of the anon folio (which is very wrong), or fail on swap/nonswap entries, failing `follow_phys()` and triggering a `WARN_ON_ONCE()` in `untrack_pfn()` and `track_pfn_copy()`, not properly calling `free_pfn_range()`.

In `free_pfn_range()`, we either wouldn't call `memtype_free()` or would call it with the wrong range, possibly leaking memory.

To fix that, let's update `follow_phys()` to refuse returning anon folios, and fallback to using the stored PFN inside `vma->vm_pgoff` for COW mappings if we run into that.

We will now properly handle `untrack_pfn()` with COW mappings, where we don't need the cachemode. We'll have to fail `fork()->track_pfn_copy()` if the first page was replaced by an anon folio, though: we'd have to store the cachemode in the VMA to make this work, likely growing the VMA size.

For now, lets keep it simple and let `track_pfn_copy()` just fail in that case: it would have failed in the past with swap/nonswap entries already, and it would have done the wrong thing with anon folios.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-237: Improper Handling of Structural Elements

### **Vulnerability CVE-2024-35884**

In the Linux kernel, the following vulnerability has been resolved:

udp: do not accept non-tunnel GSO skbs landing in a tunnel

When rx-udp-gro-forwarding is enabled UDP packets might be GROed when being forwarded. If such packets might land in a tunnel this can cause various issues and `udp_gro_receive` makes sure this isn't the case by looking for a matching socket. This is performed in `udp4/6_gro_lookup_skb` but only in the current netns. This is an issue with tunneled packets when the endpoint is in another netns. In such cases the packets will be GROed at the UDP level, which leads to various issues later on. The same thing can happen with rx-gro-list.

We saw this with geneve packets being GROed at the UDP level. In such case `gso_size` is set; later the packet goes through the geneve rx path, the geneve header is pulled, the offset are adjusted and `frag_list` skbs are not adjusted with regard to geneve. When those skbs hit `skb_fragment`, it will misbehave. Different outcomes are possible depending on what the GROed skbs look like; from corrupted packets to kernel crashes.

One example is a `BUG_ON[1]` triggered in `skb_segment` while processing the `frag_list`. Because `gso_size` is wrong (geneve header was pulled) `skb_segment` thinks there is "geneve header size" of data in `frag_list`, although it's in fact the next packet. The `BUG_ON` itself has nothing to do with the issue. This is only one of the potential issues.

Looking up for a matching socket in `udp_gro_receive` is fragile: the lookup could be extended to all netns (not speaking about performances) but nothing prevents those packets from being modified in between and we could still not find a matching socket. It's OK to keep the current logic there as it should cover most cases but we also need to make sure we handle tunnel packets being GROed too early.

This is done by extending the checks in `udp_unexpected_gso`: GSO packets lacking the `SKB_GSO_UDP_TUNNEL/_CSUM` bits and landing in a tunnel must be segmented.

[1] kernel BUG at net/core/skbuff.c:4408! RIP: 0010:skb\_segment+0xd2a/0xf70 \_\_udp\_gso\_segment+0xaa/0x560

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-923: Improper Restriction of Communication Channel to Intended Endpoints

### **Vulnerability CVE-2024-35886**

In the Linux kernel, the following vulnerability has been resolved:

ipv6: Fix infinite recursion in fib6\_dump\_done().

syzkaller reported infinite recursive calls of fib6\_dump\_done() during netlink socket destruction.

From the log, syzkaller sent an AF\_UNSPEC RTM\_GETROUTE message, and then the response was generated. The following recvmmsg() resumed the dump for IPv6, but the first call of inet6\_dump\_fib() failed at kzalloc() due to the fault injection.

```
12:01:34 executing program 3: r0 = socket
(nl_route(0x10, 0x3, 0x0) sendmsg
)nl_route(r0, ... snip ...) recvmmsg(r0, ... snip ...) (fail_nth: 8)
```

Here, fib6\_dump\_done() was set to nlk\_sk(sk)->cb.done, and the next call of inet6\_dump\_fib() set it to nlk\_sk(sk)->cb.args[3]. syzkaller stopped receiving the response halfway through, and finally netlink\_sock\_destruct() called nlk\_sk(sk)->cb.done().

fib6\_dump\_done() calls fib6\_dump\_end() and nlk\_sk(sk)->cb.done() if it is still not NULL. fib6\_dump\_end() rewrites nlk\_sk(sk)->cb.done() by nlk\_sk(sk)->cb.args[3], but it has the same function, not NULL, calling itself recursively and hitting the stack guard page.

To avoid the issue, let's set the destructor after kzalloc().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

### **Vulnerability CVE-2024-35888**

In the Linux kernel, the following vulnerability has been resolved: erspan: make sure erspan\_base\_hdr is present in skb->head.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-457: Use of Uninitialized Variable

### **Vulnerability CVE-2024-35893**

In the Linux kernel, the following vulnerability has been resolved:

net/sched: act\_skbmod: prevent kernel-infoleak

syzbot found that tcf\_skbmod\_dump() was copying four bytes from kernel stack to user space.

The issue here is that 'struct tc\_skbmod' has a four bytes hole.

We need to clear the structure before filling fields.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-908: Use of Uninitialized Resource

**Vulnerability CVE-2024-35895**

In the Linux kernel, the following vulnerability has been resolved:

bpf, sockmap: Prevent lock inversion deadlock in map delete elem

syzkaller started using corpuses where a BPF tracing program deletes elements from a sockmap/-sockhash map. Because BPF tracing programs can be invoked from any interrupt context, locks taken during a map\_delete\_elem operation must be hardirq-safe. Otherwise a deadlock due to lock inversion is possible, as reported by lockdep:

```
\lstinline|   CPU0                               CPU1
          ----                               ----
          |
```

```
lock(&htab->buckets[i].lock); local_irq_disable(); lock(&host->lock); lock(&htab->buckets[i].lock); <Inter-
rupt> lock(&host->lock);
```

Locks in sockmap are hardirq-unsafe by design. We expects elements to be deleted from sockmap/-sockhash only in task (normal) context with interrupts enabled, or in softirq context.

Detect when map\_delete\_elem operation is invoked from a context which is *not* hardirq-unsafe, that is interrupts are disabled, and bail out with an error.

Note that map updates are not affected by this issue. BPF verifier does not allow updating sockmap/-sockhash from a BPF tracing program today.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-667: Improper Locking

**Vulnerability CVE-2024-35896**

In the Linux kernel, the following vulnerability has been resolved:

netfilter: validate user input for expected length

I got multiple syzbot reports showing old bugs exposed by BPF after commit 20f2505fb436 ("bpf: Try to avoid kzalloc in cgroup/s,getsockopt")

setsockopt() @optlen argument should be taken into account before copying data.

CVSS v3.1 Base Score	7.1
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H</a>
CWE	CWE-125: Out-of-bounds Read

**Vulnerability CVE-2024-35897**

In the Linux kernel, the following vulnerability has been resolved:

netfilter: nf\_tables: discard table flag update with pending basechain deletion

Hook unregistration is deferred to the commit phase, same occurs with hook updates triggered by the table dormant flag. When both commands are combined, this results in deleting a basechain while leaving its hook still registered in the core.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-1287: Improper Validation of Specified Type of Input

### **Vulnerability CVE-2024-35898**

In the Linux kernel, the following vulnerability has been resolved:

netfilter: nf\_tables: Fix potential data-race in `__nft_flowtable_type_get()`

`nft_unregister_flowtable_type()` within `nf_flow_inet_module_exit()` can concurrent with `__nft_flowtable_type_get()` within `nf_tables_newflowtable()`. And there is not any protection when iterate over `nf_tables_flowtables` list in `__nft_flowtable_type_get()`. Therefore, there is potential data-race of `nf_tables_flowtables` list entry.

Use `list_for_each_entry_rcu()` to iterate over `nf_tables_flowtables` list in `__nft_flowtable_type_get()`, and use `rcu_read_lock()` in the caller `nft_flowtable_type_get()` to protect the entire type query process.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-35899**

In the Linux kernel, the following vulnerability has been resolved:

netfilter: nf\_tables: flush pending destroy work before `exit_net` release

Similar to 2c9f0293280e ("netfilter: nf\_tables: flush pending destroy work before netlink notifier") to address a race between `exit_net` and the destroy workqueue.

The trace below shows an element to be released via destroy workqueue while `exit_net` path (triggered via module removal) has already released the set that is used in such transaction.

CVSS v3.1 Base Score	6.1
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H</a>
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-35900**

In the Linux kernel, the following vulnerability has been resolved:

netfilter: nf\_tables: reject new basechain after table flag update

When dormant flag is toggled, hooks are disabled in the commit phase by iterating over current chains in table (existing and new).

The following configuration allows for an inconsistent state:

```
add table x add chain x y type filter hook input priority 0; add table x flags dormant; add chain x w type filter hook input priority 1;
```

which triggers the following warning when trying to unregister chain w which is already unregistered.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-1287: Improper Validation of Specified Type of Input

### **Vulnerability CVE-2024-35902**

net/rds: possible cp null dereference cp might be null, calling `cp->cp_conn` would produce null dereference. Cp is a parameter of `__rds_rdma_map` and is not reassigned.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

**Vulnerability CVE-2024-35905**

In the Linux kernel, the following vulnerability has been resolved:

bpf: Protect against int overflow for stack access size

This patch re-introduces protection against the size of access to stack memory being negative; the access size can appear negative as a result of overflowing its signed int representation. This should not actually happen, as there are other protections along the way, but we should protect against it anyway. One code path was missing such protections (fixed in the previous patch in the series), causing out-of-bounds array accesses in `check_stack_range_initialized()`. This patch causes the verification of a program with such a non-sensical access size to fail.

This check used to exist in a more indirect way, but was inadvertently removed in `a833a17aeac7`.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-129: Improper Validation of Array Index

**Vulnerability CVE-2024-35910**

In the Linux kernel, the following vulnerability has been resolved: tcp: properly terminate timers for kernel sockets We had various syzbot reports about tcp timers firing after the corresponding netns has been dismantled. Fortunately Josef Bacik could trigger the issue more often, and could test a patch I wrote two years ago. When TCP sockets are closed, we call `inet_csk_clear_xmit_timers()` to 'stop' the timers. `inet_csk_clear_xmit_timers()` can be called from any context, including when socket lock is held. This is the reason it uses `sk_stop_timer()`, aka `del_timer()`. This means that ongoing timers might finish much later. For user sockets, this is fine because each running timer holds a reference on the socket, and the user socket holds a reference on the netns. For kernel sockets, we risk that the netns is freed before timer can complete, because kernel sockets do not hold reference on the netns. This patch adds `inet_csk_clear_xmit_timers_sync()` function that using `sk_stop_timer_sync()` to make sure all timers are terminated before the kernel socket is released. Modules using kernel sockets close them in their netns `exit()` handler. Also add `sock_not_owned_by_me()` helper to get LOCKDEP support : `inet_csk_clear_xmit_timers_sync()` must not be called while socket lock is held. It is very possible we can revert in the future commit `3a58f13a881e` ("net: rds: acquire refcount on TCP sockets") which attempted to solve the issue in rds only. (`net/smc/af_smc.c` and `net/mptcp/subflow.c` have similar code) We probably can remove the `check_net()` tests from `tcp_out_of_resources()` and `__tcp_close()` in the future.

CVSS v3.1 Base Score	5.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:H</a>
CWE	CWE-665: Improper Initialization

**Vulnerability CVE-2024-35915**

nfc: nci: Fix uninit-value in `nci_dev_up` and `nci_ntf_packet`

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-908: Use of Uninitialized Resource

**Vulnerability CVE-2024-35922**

fbmon: prevent division by zero in `fb_videomode_from_videomode()`

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-369: Divide By Zero

**Vulnerability CVE-2024-35925**

block: prevent division by zero in blk\_rq\_stat\_sum()

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-369: Divide By Zero

**Vulnerability CVE-2024-35930**

scsi: lpfc: Fix possible memory leak in lpfc\_rcv\_padisc()

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-401: Missing Release of Memory after Effective Lifetime

**Vulnerability CVE-2024-35933**

Bluetooth: btintel: Fix null ptr deref in btintel\_read\_version

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-2024-35934**

net/smc: reduce rtnl pressure in smc\_pnet\_create\_pnetids\_list()

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](#)  
CWE CWE-400: Uncontrolled Resource Consumption

**Vulnerability CVE-2024-35935**

btrfs: send: handle path ref underflow in header\_iterate\_inode\_ref()

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-124: Buffer Underwrite ('Buffer Underflow')

**Vulnerability CVE-2024-35936**

btrfs: handle chunk tree lookup error in btrfs\_relocate\_sys\_chunks()

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-237: Improper Handling of Structural Elements

**Vulnerability CVE-2024-35940**

pstore/zone: Add a null pointer check to the psz\_kmsg\_read

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-2024-35944**

VMCI: Fix memcpy() run-time warning in dg\_dispatch\_as\_host()

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-787: Out-of-bounds Write

**Vulnerability CVE-2024-35950**

drm/client: Fully protect modes with dev->mode\_config.mutex

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-908: Use of Uninitialized Resource

**Vulnerability CVE-2024-35955**

kprobes: Fix possible use-after-free issue on kprobe registration

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](#)  
CWE CWE-416: Use After Free

**Vulnerability CVE-2024-35958**

net: ena: Fix incorrect descriptor free behavior

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-416: Use After Free

**Vulnerability CVE-2024-35960**

net/mlx5: Properly link new fs rules into the tree

CVSS v3.1 Base Score 9.1  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H](#)  
CWE CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-35962**

netfilter: complete validation of user input

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-1284: Improper Validation of Specified Quantity in Input

**Vulnerability CVE-2024-35965**

Bluetooth: L2CAP: Fix not validating setsockopt user input

Check user input length before copying data.

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-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

**Vulnerability CVE-2024-35966**

Bluetooth: RFCOMM: Fix not validating setsockopt user input

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-787: Out-of-bounds Write

**Vulnerability CVE-2024-35967**

Bluetooth: SCO: Fix not validating setsockopt user input

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-20: Improper Input Validation

**Vulnerability CVE-2024-35969**

ipv6: fix race condition between ipv6\_get\_ifaddr and ipv6\_del\_addr

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-770: Allocation of Resources Without Limits or Throttling

**Vulnerability CVE-2024-35973**

geneve: fix header validation in geneve\_xmit\_skb

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-908: Use of Uninitialized Resource

**Vulnerability CVE-2024-35976**

xsk: validate user input for XDP\_UMEM|COMPLETION\_FILL\_RING

CVSS v3.1 Base Score 6.7  
CVSS Vector [CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N](#)  
CWE CWE-787: Out-of-bounds Write

**Vulnerability CVE-2024-35978**

Bluetooth: Fix memory leak in hci\_req\_sync\_complete()

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-401: Missing Release of Memory after Effective Lifetime

**Vulnerability CVE-2024-35982**

batman-adv: Avoid infinite loop trying to resize local TT

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-835: Loop with Unreachable Exit Condition ('Infinite Loop')

**Vulnerability CVE-2024-35983**

bounds: Use the right number of bits for power-of-two CONFIG\_NR\_CPUS

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-20: Improper Input Validation

**Vulnerability CVE-2024-35984**

i2c: smbus: fix NULL function 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](#)  
CWE CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-35988**

riscv: Fix TASK\_SIZE on 64-bit NOMMU. On NOMMU, userspace memory can come from anywhere in physical RAM. The current definition of TASK\_SIZE is wrong if any RAM exists above 4G, causing spurious failures in the userspace access routines.

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-131: Incorrect Calculation of Buffer Size

**Vulnerability CVE-2024-35990**

dma: xilinx\_dpdma: Fix locking

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-667: Improper Locking

**Vulnerability CVE-2024-35996**

cpu: Re-enable CPU mitigations by default for !X86 architectures

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-655: Insufficient Psychological Acceptability

**Vulnerability CVE-2024-35997**

HID: i2c-hid: remove I2C\_HID\_READ\_PENDING flag to prevent lock-up

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-667: Improper Locking

**Vulnerability CVE-2024-36004**

i40e: Do not use WQ\_MEM\_RECLAIM flag for workqueue

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-404: Improper Resource Shutdown or Release

**Vulnerability CVE-2024-36005**

netfilter: nf\_tables: honor table dormant flag from netdev release event path

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-20: Improper Input Validation

**Vulnerability CVE-2024-36006**

In the Linux kernel, the following vulnerability has been resolved:

mlxsw: spectrum\_acl\_tcam: Fix incorrect list API usage

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-20: Improper Input Validation

### **Vulnerability CVE-2024-36007**

In the Linux kernel, the following vulnerability has been resolved:

mlxsw: spectrum\_acl\_tcaml: Fix warning during rehash

As previously explained, the rehash delayed work migrates filters from one region to another. This is done by iterating over all chunks (all the filters with the same priority) in the region and in each chunk iterating over all the filters.

When the work runs out of credits it stores the current chunk and entry as markers in the per-work context so that it would know where to resume the migration from the next time the work is scheduled.

Upon error, the chunk marker is reset to NULL, but without resetting the entry markers despite being relative to it. This can result in migration being resumed from an entry that does not belong to the chunk being migrated. In turn, this will eventually lead to a chunk being iterated over as if it is an entry. Because of how the two structures happen to be defined, this does not lead to KASAN splats, but to warnings such as.

Fix by creating a helper that resets all the markers and call it from all the places the currently only reset the chunk marker. For good measures also call it when starting a completely new rehash. Add a warning to avoid future cases.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-36008**

In the Linux kernel, the following vulnerability has been resolved:

ipv4: check for NULL idev in ip\_route\_use\_hint()

syzbot was able to trigger a NULL deref in fib\_validate\_source() in an old tree.

It appears the bug exists in latest trees.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

### **Vulnerability CVE-2024-36020**

In the Linux kernel, the following vulnerability has been resolved:

i40e: fix vf may be used uninitialized in this function warning

To fix the regression introduced by commit 52424f974bc5, which causes servers hang in very hard to reproduce conditions with resets races. Using two sources for the information is the root cause. In this function before the fix bumping v didn't mean bumping vf pointer. But the code used this variables interchangeably, so stale vf could point to different/not intended vf.

Remove redundant "v" variable and iterate via single VF pointer across whole function instead to guarantee VF pointer validity.

CVSS v3.1 Base Score	5.3
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-36270**

netfilter: tproxy: bail out if IP has been disabled on the device syzbot reports: general protection fault, probably for non-canonical address

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-20: Improper Input Validation

### **Vulnerability CVE-2024-36286**

In the Linux kernel, the following vulnerability has been resolved: netfilter: nfnetlink\_queue: acquire rcu\_read\_lock() in instance\_destroy\_rcu().

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-1287: Improper Validation of Specified Type of Input

### **Vulnerability CVE-2024-36288**

SUNRPC: Fix loop termination condition in gss\_free\_in\_token\_pages() The in\_token->pages[] array is not NULL terminated. This results in the following KASAN splat: KASAN: maybe wild-memory-access in range [0x04a2013400000008-0x04a201340000000f].

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

### **Vulnerability CVE-2024-36484**

In the Linux kernel, the following vulnerability has been resolved: net: relax socket state check at accept time.

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-99: Improper Control of Resource Identifiers ('Resource Injection')

### **Vulnerability CVE-2024-36489**

tls: missing memory barrier in tls\_init. In tls\_init(), a write memory barrier is missing, and store-store reordering may cause NULL dereference in tls\_setsockopt,getsockopt.

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-20: Improper Input Validation

### **Vulnerability CVE-2024-36894**

In the Linux kernel, the following vulnerability has been resolved: usb: gadget: f\_fs: Fix race between aio\_cancel() and AIO request complete

CVSS v3.1 Base Score 4.4  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H](#)  
CWE CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

**Vulnerability CVE-2024-36899**

In the Linux kernel, the following vulnerability has been resolved:

gpiolib: cdev: Fix use after free in lineinfo\_changed\_notify

The use-after-free issue occurs as follows: when the GPIO chip device file is being closed by invoking `gpio_chrdev_release()`, `watched_lines` is freed by `bitmap_free()`, but the unregistration of `lineinfo_changed_nb` notifier chain failed due to waiting write `rwsem`. Additionally, one of the GPIO chip's lines is also in the release process and holds the notifier chain's read `rwsem`. Consequently, a race condition leads to the use-after-free of `watched_lines`.

CVSS v3.1 Base Score	7.0
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

**Vulnerability CVE-2024-36902**

Vulnerability in Linux kernel: ipv6: fib6\_rules: avoid possible NULL dereference in `fib6_rule_action()` syzbot is able to trigger the following crash [1], caused by unsafe `ip6_dst_idev()` use. Indeed `ip6_dst_idev()` can return NULL, and must always be checked.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-36904**

In the Linux kernel, the following vulnerability has been resolved: tcp: Use `refcount_inc_not_zero()` in `tcp_twsk_unique()`.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-416: Use After Free

**Vulnerability CVE-2024-36905**

In the Linux kernel, the following vulnerability has been resolved: tcp: defer shutdown(`SEND_SHUTDOWN`) for `TCP_SYN_RECV` sockets.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-369: Divide By Zero

**Vulnerability CVE-2024-36916**

In the Linux kernel, the following vulnerability has been resolved: blk-iocost: avoid out of bounds shift UBSAN catches undefined behavior in `blk-iocost`, where sometimes `iocg->delay` is shifted right by a number that is too large, resulting in undefined behavior on some architectures. [ 186.556576] \_\_\_\_\_[ cut here ]\_\_\_\_\_ UBSAN: shift-out-of-bounds in block/blk-iocost.c:1366:23 shift exponent 64 is too large for 64-bit type 'u64' (aka 'unsigned long long') CPU: 16 PID: 0 Comm: swapper/16 Tainted: G S E N 6.9.0-0\_fbk700\_debug\_rc2\_kbuilder\_0\_gc85af715cac0 #1 Hardware name: Quanta Twin Lakes MP/Twin Lakes Passive MP, BIOS F09\_3A23 12/08/2020 Call Trace: <IRQ> dump\_stack\_lvl+0x8f/0xe0 \_\_ubsan\_handle\_shift\_out\_of\_bounds+0x22c/0x280 iocg\_kick\_delay+0x30b/0x310 ioc\_timer\_fn+0x2fb/0x1f80 \_\_run\_timer\_base+0x1b6/0x250 ... Avoid that undefined behavior by simply taking the "delay = 0" branch if the shift is too large. I am not sure what the symptoms of an undefined value delay will be, but I suspect it could be more than a little annoying to debug.

CVSS v3.1 Base Score	6.5
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L</a>
CWE	CWE-787: Out-of-bounds Write

**Vulnerability CVE-2024-36929**

In the Linux kernel, the following vulnerability has been resolved: net: core: reject skb\_copy(\_expand) for fraglist GSO skbs SKB\_GSO\_FRAGLIST skbs must not be linearized, otherwise they become invalid. Return NULL if such an skb is passed to skb\_copy or skb\_copy\_expand, in order to prevent a crash on a potential later call to skb\_gso\_segment.

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-237: Improper Handling of Structural Elements

**Vulnerability CVE-2024-36939**

In the Linux kernel, the following vulnerability has been resolved: nfs: Handle error of rpc\_proc\_register() in nfs\_net\_init(). syzkaller reported a warning [0] triggered while destroying immature netns. rpc\_proc\_register() was called in init\_nfs\_fs(), but its error has been ignored since at least the initial commit 1da177e4c3f4 ("Linux-2.6.12-rc2"). Recently, commit d47151b79e32 ("nfs: expose /proc/net/sunrpc/nfs in net namespaces") converted the procs to per-netns and made the problem more visible. Even when rpc\_proc\_register() fails, nfs\_net\_init() could succeed, and thus nfs\_net\_exit() will be called while destroying the netns. Then, remove\_proc\_entry() will be called for non-existing proc directory and trigger the warning below. Let's handle the error of rpc\_proc\_register() properly in nfs\_net\_init(). [0]: name 'nfs' WARNING: CPU: 1 PID: 1710 at fs/proc/generic.c:711 remove\_proc\_entry+0x1bb/0x2d0 fs/proc/generic.c:711 Modules linked in: CPU: 1 PID: 1710 Comm: syz-executor.2 Not tainted 6.8.0-12822-gcd51db110a7e #12 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 RIP: 0010:remove\_proc\_entry+0x1bb/0x2d0 fs/proc/generic.c:711 Code: 41 5d 41 5e c3 e8 85 09 b5 ff 48 c7 c7 88 58 64 86 e8 09 0e 71 02 e8 74 09 b5 ff 4c 89 e6 48 c7 c7 de 1b 80 84 e8 c5 ad 97 ff <0f> 0b eb b1 e8 5c 09 b5 ff 48 c7 c7 88 58 64 86 e8 e0 0d 71 02 eb RSP: 0018:ffffc9000c6d7ce0 EFLAGS: 00010286 RAX: 0000000000000000 RBX: ffff8880422b8b00 RCX: ffffffff8110503c RDX: ffff888030652f00 RSI: ffffffff81105045 RDI: 0000000000000001 RBP: 0000000000000000 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000000000001 R11: ffffffff81bb62cb R12: ffffffff84807ffc R13: ffff88804ad6fcc0 R14: ffffffff84807ffc R15: ffffffff85741ff8 FS: 00007f30cfba8640(0000) GS:ffff88807dd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ff51afe8000 CR3: 000000005a60a005 CR4: 0000000000770ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> rpc\_proc\_unregister+0x64/0x70 net/sunrpc/stats.c:310 nfs\_net\_exit+0x1c/0x30 fs/nfs/inode.c:2438 ops\_exit\_list+0x62/0xb0 net/core/net\_namespace.c:170 setup\_net+0x46c/0x660 net/core/net\_namespace.c:372 copy\_net\_ns+0x244/0x590 net/core/net\_namespace.c:505 create\_new\_namespaces+0x2ed/0x770 kernel/nsproxy.c:110 unshare\_nsproxy\_namespaces+0xae/0x160 kernel/nsproxy.c:228 ksys\_unshare+0x342/0x760 kernel/fork.c:3322 \_\_do\_sys\_unshare kernel/fork.c:3393 [inline] \_\_se\_sys\_unshare kernel/fork.c:3391 [inline] \_\_x64\_sys\_unshare+0x1f/0x30 kernel/fork.c:3391 do\_syscall\_x64 arch/x86/entry/common.c:52 [inline] do\_syscall\_64+0x4f/0x110 arch/x86/entry/common.c:83 entry\_SYSCALL\_64\_after\_hwframe+0x46/0x4e RIP: 0033:0x7f30d0febe5d Code: ff c3 66 2e 0f 1f 84 00 00 00 00 90 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 73 9f 1b 00 f7 d8 64 89 01 48 RSP: 002b:00007f30cfba7cc8 EFLAGS: 00000246 ORIG\_RAX: 0000000000000110 RAX: ffffffff85741ff8 RBX: 00000000004bbf80 RCX: 00007f30d0febe5d RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000006c020600 RBP: 00000000004bbf80 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000002 R13: 000000000000000b R14: 00007f30d104c530 R15: 0000000000000000 </TASK>

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-391: Unchecked Error Condition

**Vulnerability CVE-2024-36940**

In the Linux kernel, the following vulnerability has been resolved: pinctrl: core: delete incorrect free in pinctrl\_enable() The "pctldev" struct is allocated in devm\_pinctrl\_register\_and\_init(). It's a devm\_managed pointer that is freed by devm\_pinctrl\_dev\_release(), so freeing it in pinctrl\_enable() will lead to a double free. The devm\_pinctrl\_dev\_release() function frees the pindescs and destroys the mutex as well.

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-415: Double Free

**Vulnerability CVE-2024-36959**

In the Linux kernel, the following vulnerability has been resolved: pinctrl: devicetree: fix refcount leak in pinctrl\_dt\_to\_map() If we fail to allocate proptype buffer, we need to drop the reference count we just took. Because the pinctrl\_dt\_free\_maps() includes the dropping operation, here we call it directly.

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-668: Exposure of Resource to Wrong Sphere

**Vulnerability CVE-2024-36974**

net/sched: taprio: always validate TCA\_TAPRIO\_ATTR\_PRIOMAP. If one TCA\_TAPRIO\_ATTR\_PRIOMAP attribute has been provided, taprio\_parse\_mqprio\_opt() must validate it, or userspace can inject arbitrary data to the kernel, the second time taprio\_change() is called. First call (with valid attributes) sets dev->num\_tc to a non zero value. Second call (with arbitrary mqprio attributes) returns early from taprio\_parse\_mqprio\_opt() and bad things can happen.

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-20: Improper Input Validation

**Vulnerability CVE-2024-36978**

net: sched: sch\_multiq: possible OOB write in multiq\_tune() q->bands will be assigned to qopt->bands to execute subsequent code logic after kcalloc. So the old q->bands should not be used in kcalloc. Otherwise, an out-of-bounds write will occur.

CVSS v3.1 Base Score 6.1  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-37356**

In the Linux kernel, the following vulnerability has been resolved: tcp: Fix shift-out-of-bounds in dctcp\_update\_alpha().

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](#)  
CWE CWE-125: Out-of-bounds Read

**Vulnerability CVE-2024-38381**

nfc: nci: Fix uninit-value in nci\_rx\_work syzbot reported the following uninit-value access issue [1] nci\_rx\_work() parses received packet from ndev->rx\_q. It should be validated header size, payload size and total packet size before processing the packet. If an invalid packet is detected, it should be silently discarded.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38547**

media: atomisp: ssh\_css: null-pointer dereference in load\_video\_binaries.

CVSS v3.1 Base Score 4.4  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-38552**

drm/amd/display: Fix potential index out of bounds in color transformation function Fixes index out of bounds issue in the color transformation function. The issue could occur when the index 'i' exceeds the number of transfer function points (TRANSFER\_FUNC\_POINTS). The fix adds a check to ensure 'i' is within bounds before accessing the transfer function points. If 'i' is out of bounds, an error message is logged and the function returns false to indicate an error.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38558**

net: openvswitch: fix overwriting ct original tuple for ICMPv6 OVS\_PACKET\_CMD\_EXECUTE has 3 main attributes: - OVS\_PACKET\_ATTR\_KEY - Packet metadata in a netlink format. - OVS\_PACKET\_ATTR\_PACKET - Binary packet content. - OVS\_PACKET\_ATTR\_ACTIONS - Actions to execute on the packet. OVS\_PACKET\_ATTR\_KEY is parsed first to populate sw\_flow\_key structure with the metadata like contrack state, input port, recirculation id, etc.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38559**

scsi: qedf: Ensure the copied buf is NUL terminated Currently, we allocate a count-sized kernel buffer and copy count from userspace to that buffer. Later, we use kstrtouint on this buffer but we don't ensure that the string is terminated inside the buffer, this can lead to OOB read when using kstrtouint.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38560**

scsi: bfa: Ensure the copied buf is NUL terminated Currently, we allocate a nbytes-sized kernel buffer and copy nbytes from userspace to that buffer. Later, we use sscanf on this buffer but we don't ensure that the string is terminated inside the buffer, this can lead to OOB read when using sscanf.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38565**

wifi: ar5523: enable proper endpoint verification Syzkaller reports [1] hitting a warning about an endpoint in use not having an expected type to it. Fix the issue by checking for the existence of all proper endpoints with their according types intact. Sadly, this patch has not been tested on real hardware.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38567**

wifi: carl9170: add a proper sanity check for endpoints Syzkaller reports [1] hitting a warning which is caused by presence of a wrong endpoint type at the URB sumbitting stage. While there was a check for a specific 4th endpoint, since it can switch types between bulk and interrupt, other endpoints are trusted implicitly. Similar warning is triggered in a couple of other syzbot issues [2].

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-20: Improper Input Validation

**Vulnerability CVE-2024-38578**

ecryptfs: Fix buffer size for tag 66 packet The 'TAG 66 Packet Format' description is missing the cipher code and checksum fields that are packed into the message packet. As a result, the buffer allocated for the packet is 3 bytes too small and write\_tag\_66\_packet() will write up to 3 bytes past the end of the buffer. Fix this by increasing the size of the allocation so the whole packet will always fit in the buffer.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38579**

crypto: bcm - Fix pointer arithmetic In spu2\_dump\_omd() value of ptr is increased by ciph\_key\_len instead of hash\_iv\_len which could lead to going beyond the buffer boundaries.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38587**

In the Linux kernel, the following vulnerability has been resolved:

speakup: Fix sizeof() vs ARRAY\_SIZE() bug

The "buf" pointer is an array of u16 values. This code should be using ARRAY\_SIZE() (which is 256) instead of sizeof() (which is 512), otherwise it can the still got out of bounds.

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](#)  
CWE CWE-129: Improper Validation of Array Index

**Vulnerability CVE-2024-38589**

netrom: fix possible dead-lock in nr\_rt\_ioctl() syzbot loves netrom, and found a possible deadlock in nr\_rt\_ioctl [1] Make sure we always acquire nr\_node\_list\_lock before nr\_node\_lock(nr\_node).

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-20: Improper Input Validation

**Vulnerability CVE-2024-38596**

In the Linux kernel, the following vulnerability has been resolved: af\_unix: Fix data races in unix\_release\_sock/unix\_stream\_sendmsg.

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](#)  
CWE CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

**Vulnerability CVE-2024-38598**

In the Linux kernel, the following vulnerability has been resolved: md: fix resync softlockup when bitmap size is less than array size.

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-667: Improper Locking

**Vulnerability CVE-2024-38599**

jffs2: prevent xattr node from overflowing the eraseblock Add a check to make sure that the requested xattr node size is no larger than the eraseblock minus the cleanmarker. Unlike the usual inode nodes, the xattr nodes aren't split into parts and spread across multiple eraseblocks, which means that a xattr node must not occupy more than one eraseblock. If the requested xattr value is too large, the xattr node can spill onto the next eraseblock, overwriting the nodes and causing errors.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38612**

In the Linux kernel, the following vulnerability has been resolved: ipv6: sr: fix invalid unregister error path The error path of seg6\_init() is wrong in case CONFIG\_IPV6\_SEG6\_LWTUNNEL is not defined. In that case if seg6\_hmac\_init() fails, the genl\_unregister\_family() isn't called. This issue exist since commit 46738b1317e1 ("ipv6: sr: add option to control lwtunnel support"), and commit 5559cea2d5aa ("ipv6: sr: fix possible use-after-free and null-ptr-deref") replaced unregister\_pernet\_subsys() with genl\_unregister\_family() in this error path.

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-459: Incomplete Cleanup

**Vulnerability CVE-2024-38615**

cpufreq: exit() callback is optional The exit() callback is optional and shouldn't be called without checking a valid pointer first. Also, we must clear freq\_table pointer even if the exit() callback isn't present.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38619**

usb-storage: alauda: Check whether the media is initialized. The member "uzonesize" of struct alauda\_info will remain 0 if alauda\_init\_media() fails, potentially causing divide errors in alauda\_read\_data() and alauda\_write\_lba().

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-20: Improper Input Validation

**Vulnerability CVE-2024-38635**

soundwire: cadence: invalid PDI offset.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38659**

enic: Validate length of nl attributes in enic\_set\_vf\_port enic\_set\_vf\_port assumes that the nl attribute IFLA\_PORT\_PROFILE is of length PORT\_PROFILE\_MAX and that the nl attributes IFLA\_PORT\_INSTANCE\_UUID, IFLA\_PORT\_HOST\_UUID are of length PORT\_UUID\_MAX. These attributes are validated (in the function do\_setlink in rtnetlink.c) using the nla\_policy ifla\_port\_policy. The policy defines IFLA\_PORT\_PROFILE as NLA\_STRING, IFLA\_PORT\_INSTANCE\_UUID as NLA\_BINARY and IFLA\_PORT\_HOST\_UUID as NLA\_STRING. That means that the length validation using the policy is for the max size of the attributes and not on exact size so the length of these attributes might be less than the sizes that enic\_set\_vf\_port expects. This might cause an out of bounds read access in the memcpys of the data of these attributes in enic\_set\_vf\_port.

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-20: Improper Input Validation

**Vulnerability CVE-2024-38662**

bpf: Allow delete from sockmap/sockhash only if update is allowed. We have seen an influx of syzkaller reports where a BPF program attached to a tracepoint triggers a locking rule violation by performing a map\_delete on a sockmap/sockhash. We don't intend to support this artificial use scenario. Extend the existing verifier allowed-program-type check for updating sockmap/sockhash to also cover deleting from a map. From now on only BPF programs which were previously allowed to update sockmap/sockhash can delete from these map types.

CVSS v3.1 Base Score 4.4  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-38780**

In the Linux kernel, the following vulnerability has been resolved: dma-buf/sw-sync: don't enable IRQ from sync\_print\_obj().

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-667: Improper Locking

**Vulnerability CVE-2024-39468**

smb: client: Deadlock in smb2\_find\_smb\_tcon().

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-20: Improper Input Validation

**Vulnerability CVE-2024-39482**

bcache: Variable length array abuse in btree\_iter.

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-20: Improper Input Validation

**Vulnerability CVE-2024-39489**

In the Linux kernel, the following vulnerability has been resolved: ipv6: sr: fix memleak in seg6\_hmac\_init\_algo seg6\_hmac\_init\_algo returns without cleaning up the previous allocations if one fails, so it's going to leak all that memory and the crypto tfms. Update seg6\_hmac\_exit to only free the memory when allocated, so we can reuse the code directly.

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-401: Missing Release of Memory after Effective Lifetime

**Vulnerability CVE-2024-39493**

In the Linux kernel, the following vulnerability has been resolved:

crypto: qat - Fix ADF\_DEV\_RESET\_SYNC memory leak

Using completion\_done to determine whether the caller has gone away only works after a complete call. Furthermore it's still possible that the caller has not yet called wait\_for\_completion, resulting in another potential UAF.

Fix this by making the caller use cancel\_work\_sync and then freeing the memory safely.

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-401: Missing Release of Memory after Effective Lifetime

**Vulnerability CVE-2024-39502**

ionic: use after netif\_napi\_del(). When queues are started, netif\_napi\_add() and napi\_enable() are called. If there are 4 queues and only 3 queues are used for the current configuration, only 3 queues' napi should be registered and enabled. The ionic\_qcq\_enable() checks whether the .poll pointer is not NULL for enabling only the using queue' napi. Unused queues' napi will not be registered by netif\_napi\_add(), so the .poll pointer indicates NULL. But it couldn't distinguish whether the napi was unregistered or not because netif\_napi\_del() doesn't reset the .poll pointer to NULL. So, ionic\_qcq\_enable() calls napi\_enable() for the queue, which was unregistered by netif\_napi\_del().

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-416: Use After Free

**Vulnerability CVE-2024-39503**

netfilter: ipset: race between namespace cleanup and gc in the list:set type. The namespace cleanup can destroy the list:set type of sets while the gc of the set type is waiting to run in rcu cleanup. The latter uses data from the destroyed set which thus leads use after free.

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-416: Use After Free

**Vulnerability CVE-2024-39509**

HID: core: remove unnecessary WARN\_ON() in implement(). There is a warning in a call to implement() when trying to write a value into a field of smaller size in an output report. Since implement() already has a warn message printed out with the help of hid\_warn() and value in question gets trimmed with: ... value &= m; ... WARN\_ON may be considered superfluous.

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-20: Improper Input Validation

### **Vulnerability CVE-2024-40905**

ipv6: possible race in \_\_fib6\_drop\_pcpu\_from().

CVSS v3.1 Base Score	4.4
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-40912**

wifi: mac80211: deadlock in ieee80211\_sta\_ps\_deliver\_wakeup().

CVSS v3.1 Base Score	4.7
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-40916**

drm/exynos: hdmi: report safe 640x480 mode as a fallback when no EDID found When reading EDID fails and driver reports no modes available, the DRM core adds an artificial 1024x786 mode to the connector.

CVSS v3.1 Base Score	4.4
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-40934**

HID: logitech-dj: Fix memory leak in logi\_dj\_rcv\_switch\_to\_dj\_mode() Fix a memory leak on logi\_dj\_rcv\_send\_report() error path.

CVSS v3.1 Base Score	4.4
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L</a>
CWE	CWE-404: Improper Resource Shutdown or Release

### **Vulnerability CVE-2024-40941**

wifi: iwlmwifi: mvm: don't read past the mfuart notification. In case the firmware sends a notification that claims it has more data than it has, it will read past that was allocated for the notification.

CVSS v3.1 Base Score	4.1
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-125: Out-of-bounds Read

### **Vulnerability CVE-2024-40942**

wifi: mac80211: mesh: Fix leak of mesh\_preq\_queue objects The hwmp code use objects of type mesh\_preq\_queue, added to a list in ieee80211\_if\_mesh, to keep track of mpath we need to resolve. If the mpath gets deleted, ex mesh interface is removed, the entries in that list will never get cleaned.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-402: Transmission of Private Resources into a New Sphere ('Resource Leak')

**Vulnerability CVE-2024-40945**

iommu: Return right value in iommu\_sva\_bind\_device() iommu\_sva\_bind\_device() should return either a sva bond handle or an ERR\_PTR value in error cases. Existing drivers (idxd and uacce) only check the return value with IS\_ERR(). This could potentially lead to a kernel NULL pointer dereference issue if the function returns NULL instead of an error pointer. In reality, this doesn't cause any problems because iommu\_sva\_bind\_device() only returns NULL when the kernel is not configured with CONFIG\_IOMMU\_SVA.

CVSS v3.1 Base Score 6.8  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H](#)  
CWE CWE-393: Return of Wrong Status Code

**Vulnerability CVE-2024-40958**

netns: Make get\_net\_ns() handle zero refcount net Syzkaller hit a warning: refcount\_t: addition on 0; use-after-free.

CVSS v3.1 Base Score 4.0  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N](#)  
CWE CWE-416: Use After Free

**Vulnerability CVE-2024-40959**

In the Linux kernel, the following vulnerability has been resolved: xfrm6: check ip6\_dst\_idev() return value in xfrm6\_get\_saddr().

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-2024-40960**

ipv6: prevent possible NULL dereference in rt6\_probe() syzbot caught a NULL dereference in rt6\_probe() [1] Bail out if \_\_in6\_dev\_get() returns NULL.

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-2024-40961**

ipv6: prevent possible NULL deref in fib6\_nh\_init() syzbot reminds us that in6\_dev\_get() can return NULL.

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-2024-40971**

f2fs: remove clear SB\_INLINECRYPT flag in default\_options In f2fs\_remount, SB\_INLINECRYPT flag will be clear and re-set. If create new file or open file during this gap, these files will not use inlinecrypt. Worse case, it may lead to data corruption if wrappedkey\_v0 is enable.

CVSS v3.1 Base Score 4.0  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-40978**

scsi: qedi: crash while reading debugfs attribute. The qedi\_dbg\_do\_not\_recover\_cmd\_read() function invokes sprintf() directly on a \_\_user pointer, which results into the crash.

CVSS v3.1 Base Score 6.2  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-40980**

drop\_monitor: replace spin\_lock by raw\_spin\_lock trace\_drop\_common() is called with preemption disabled, and it acquires a spin\_lock. This is problematic for RT kernels because spin\_locks are sleeping locks in this configuration, which causes the following splat.

CVSS v3.1 Base Score 5.9  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-40984**

ACPICA: Revert "ACPICA: avoid Info: mapping multiple BARs. Your kernel is fine."

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-2024-40993**

netfilter: ipset: suspicious rcu\_dereference\_protected().

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-20: Improper Input Validation

**Vulnerability CVE-2024-40995**

net/sched: act\_api: possible infinite loop in tcf\_idr\_check\_alloc().

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-20: Improper Input Validation

**Vulnerability CVE-2024-41000**

block/ioctl: prefer different overflow check Running syzkaller with the newly reintroduced signed integer overflow sanitizer.

CVSS v3.1 Base Score 5.9  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L](#)  
CWE CWE-190: Integer Overflow or Wraparound

**Vulnerability CVE-2024-41004**

tracing: Build event generation tests only as modules The kprobes and synth event generation test modules add events and lock (get a reference) those event file reference in module init function, and unlock and delete it in module exit function. This is because those are designed for playing as modules. If we make those modules as built-in, those events are left locked in the kernel, and never be removed.

CVSS v3.1 Base Score 5.9  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-41005**

netpoll: race condition in netpoll\_owner\_active KCSAN detected a race condition in netpoll.

CVSS v3.1 Base Score 4.9  
CVSS Vector [CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L](#)  
CWE CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

**Vulnerability CVE-2024-41006**

netrom: a memory leak in nr\_heartbeat\_expiry().

CVSS v3.1 Base Score 4.4  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L](#)  
CWE CWE-404: Improper Resource Shutdown or Release

**Vulnerability CVE-2024-41016**

ocfs2: strict bound check before memcmp in ocfs2\_xattr\_find\_entry()

xattr in ocfs2 maybe 'non-indexed', which saved with additional space requested. It's better to check if the memory is out of bound before memcmp, although this possibility mainly comes from crafted poisonous images.

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:H/A:N](#)  
CWE CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

**Vulnerability CVE-2024-41996**

Validating the order of the public keys in the Diffie-Hellman Key Agreement Protocol, when an approved safe prime is used, allows remote attackers (from the client side) to trigger unnecessarily expensive server-side DHE modular-exponentiation calculations. The client may cause asymmetric resource consumption. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE and validate the order of the public key.

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](#)  
CWE CWE-295: Improper Certificate Validation

**Vulnerability CVE-2024-42070**

In the Linux kernel, the following vulnerability has been resolved: netfilter: nf\_tables: fully validate NFT\_DATA\_VALUE on store to data registers register store validation for NFT\_DATA\_VALUE is conditional, however, the datatype is always either NFT\_DATA\_VALUE or NFT\_DATA\_VERDICT. This only requires a new helper function to infer the register type from the set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be leaked through the registers.

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-401: Missing Release of Memory after Effective Lifetime

**Vulnerability CVE-2024-42082**

xdp: unused WARN() in \_\_xdp\_reg\_mem\_model().

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-770: Allocation of Resources Without Limits or Throttling

**Vulnerability CVE-2024-42090**

pinctrl: deadlock in create\_pinctrl() when handling -EPROBE\_DEFER. In create\_pinctrl(), pinctrl\_maps\_mutex is acquired before calling add\_setting(). If add\_setting() returns -EPROBE\_DEFER, create\_pinctrl() calls pinctrl\_free(). However, pinctrl\_free() attempts to acquire pinctrl\_maps\_mutex, which is already held by create\_pinctrl(), leading to a potential deadlock.

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-833: Deadlock

**Vulnerability CVE-2024-42093**

net/dpaa2: explicit cpumask var allocation on stack For CONFIG\_CPUMASK\_OFFSTACK=y kernel, explicit allocation of cpumask variable on stack can cause potential stack overflow.

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](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-42094**

net/iucv: explicit cpumask var allocation on stack For CONFIG\_CPUMASK\_OFFSTACK=y kernel, explicit allocation of cpumask variable on stack can cause potential stack overflow.

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](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-42096**

In the Linux kernel, the following vulnerability has been resolved: x86: stop playing stack games in profile\_pc().

CVSS v3.1 Base Score 5.1  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:H](#)  
CWE CWE-125: Out-of-bounds Read

**Vulnerability CVE-2024-42097**

A missed validation vulnerability in the Linux Kernel's MIDI sequencer and router support functionality could allow a local user to crash the system.

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](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-42114**

wifi: cfg80211: restrict NL80211\_ATTR\_TXQ\_QUANTUM values

CVSS v3.1 Base Score 4.4  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H](#)  
CWE CWE-667: Improper Locking

### **Vulnerability CVE-2024-42259**

In the Linux kernel, the following vulnerability has been resolved:

drm/i915/gem: Fix Virtual Memory mapping boundaries calculation

Calculating the size of the mapped area as the lesser value between the requested size and the actual size does not consider the partial mapping offset. This can cause page fault access.

Fix the calculation of the starting and ending addresses, the total size is now deduced from the difference between the end and start addresses.

Additionally, the calculations have been rewritten in a clearer and more understandable form.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-131: Incorrect Calculation of Buffer Size

### **Vulnerability CVE-2024-42265**

In the Linux kernel, the following vulnerability has been resolved:

protect the fetch of `->fd[fd]` in `do_dup2()` from mispredictions

both callers have verified that `fd` is not greater than `->max_fds`; however, misprediction might end up with `tofree = fdt->fd[fd]`; being speculatively executed. That's wrong for the same reasons why it's wrong in `close_fd()/file_close_fd_locked()`; the same solution applies - `array_index_nospec(fd, fdt->max_fds)` could differ from `fd` only in case of speculative execution on mispredicted path.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-99: Improper Control of Resource Identifiers ('Resource Injection')

### **Vulnerability CVE-2024-42272**

sched: `act_ct`: take care of padding in struct `zones_ht_key`.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-42276**

In the Linux kernel, the following vulnerability has been resolved:

nvme-pci: add missing condition check for existence of mapped data

`nvme_map_data()` is called when request has physical segments, hence the `nvme_unmap_data()` should have same condition to avoid dereference.

CVSS v3.1 Base Score	4.4
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-42281**

In the Linux kernel, the following vulnerability has been resolved:

bpf: Fix a segment issue when downgrading gso\_size

Linearize the skb when downgrading gso\_size because it may trigger a BUG\_ON() later when the skb is segmented as described in [1,2].

CVSS v3.1 Base Score	5.1
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H</a>
CWE	CWE-20: Improper Input Validation

**Vulnerability CVE-2024-42283**

In the Linux kernel, the following vulnerability has been resolved:

net: nexthop: Initialize all fields in dumped nexthops

struct nexthop\_grp contains two reserved fields that are not initialized by nla\_put\_nh\_group(), and carry garbage. This can be observed e.g. with strace (edited for clarity):

```
\lstinline|# ip nexthop add id 1 dev lo
# ip nexthop add id 101 group 1
# strace -e recvmsg ip nexthop get id 101
\dots
recvmsg(\dots [{nla_len=12, nla_type=NHA_GROUP},
               [{id=1, weight=0, resvd1=0x69, resvd2=0x67}]] \dots) = 52
|
```

The fields are reserved and therefore not currently used. But as they are, they leak kernel memory, and the fact they are not just zero complicates repurposing of the fields for new ends. Initialize the full structure.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-908: Use of Uninitialized Resource

**Vulnerability CVE-2024-42292**

In the Linux kernel, the following vulnerability has been resolved:

kobject\_uevent: Fix OOB access within zap\_modalias\_env()

zap\_modalias\_env() wrongly calculates size of memory block to move, so will cause OOB memory access issue if variable MODALIAS is not the last one within its @env parameter, fixed by correcting size to memmove.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

### **Vulnerability CVE-2024-42302**

In the Linux kernel, the following vulnerability has been resolved:

PCI/DPC: Fix use-after-free on concurrent DPC and hot-removal

Keith reports a use-after-free when a DPC event occurs concurrently to hot-removal of the same portion of the hierarchy:

The `dpc_handler()` awaits readiness of the secondary bus below the Downstream Port where the DPC event occurred. To do so, it polls the config space of the first child device on the secondary bus. If that child device is concurrently removed, accesses to its struct `pci_dev` cause the kernel to oops.

That's because `pci_bridge_wait_for_secondary_bus()` neglects to hold a reference on the child device. Before v6.3, the function was only called on resume from system sleep or on runtime resume. Holding a reference wasn't necessary back then because the `pciehp` IRQ thread could never run concurrently. (On resume from system sleep, IRQs are not enabled until after the `resume_noirq` phase. And runtime resume is always awaited before a PCI device is removed.)

However starting with v6.3, `pci_bridge_wait_for_secondary_bus()` is also called on a DPC event. Commit `53b54ad074de` ("PCI/DPC: Await readiness of secondary bus after reset"), which introduced that, failed to appreciate that `pci_bridge_wait_for_secondary_bus()` now needs to hold a reference on the child device because `dpc_handler()` and `pciehp` may indeed run concurrently. The commit was backported to v5.10+ stable kernels, so that's the oldest one affected.

Add the missing reference acquisition.

Abridged stack trace:

```
BUG: unable to handle page fault for address: 00000000091400c0 CPU: 15 PID: 2464
Comm: irq/53-pcie-dpc 6.9.0 RIP: pci_bus_read_config_dword+0x17/0x50 pci_dev_wait()
pci_bridge_wait_for_secondary_bus() dpc_reset_link() pcie_do_recovery() dpc_handler()
```

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2024-42304**

In the Linux kernel, the following vulnerability has been resolved:

ext4: make sure the first directory block is not a hole

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-42305**

In the Linux kernel, the following vulnerability has been resolved:

ext4: check dot and dotdot of `dx_root` before making dir indexed

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-125: Out-of-bounds Read

### **Vulnerability CVE-2024-42306**

In the Linux kernel, the following vulnerability has been resolved:

udf: Avoid using corrupted block bitmap buffer

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-42312**

In the Linux kernel, the following vulnerability has been resolved:

sysctl: always initialize i\_uid/i\_gid

Always initialize i\_uid/i\_gid inside the sysfs core so set\_ownership() can safely skip setting them.

Commit 5ec27ec735ba ("fs/proc/proc\_sysctl.c: fix the default values of i\_uid/i\_gid on /proc/sys inodes.") added defaults for i\_uid/i\_gid when set\_ownership() was not implemented. It also missed adjusting net\_ctl\_set\_ownership() to use the same default values in case the computation of a better value failed.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-43828**

In the Linux kernel, the following vulnerability has been resolved:

ext4: fix infinite loop when replaying fast\_commit

When doing fast\_commit replay an infinite loop may occur due to an uninitialized extent\_status struct. ext4\_ext\_determine\_insert\_hole() does not detect the replay and calls ext4\_es\_find\_extent\_range(), which will return immediately without initializing the 'es' variable.

Because 'es' contains garbage, an integer overflow may happen causing an infinite loop in this function, easily reproducible using fstest generic/039.

This commit fixes this issue by unconditionally initializing the structure in function ext4\_es\_find\_extent\_range().

Thanks to Zhang Yi, for figuring out the real problem!

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

### **Vulnerability CVE-2024-43830**

In the Linux kernel, the following vulnerability has been resolved:

leds: trigger: Unregister sysfs attributes before calling deactivate()

Triggers which have trigger specific sysfs attributes typically store related data in trigger-data allocated by the activate() callback and freed by the deactivate() callback.

Calling device\_remove\_groups() after calling deactivate() leaves a window where the sysfs attributes show/store functions could be called after deactivation and then operate on the just freed trigger-data.

Move the device\_remove\_groups() call to before deactivate() to close this race window.

This also makes the deactivation path properly do things in reverse order of the activation path which calls the activate() callback before calling device\_add\_groups().

CVSS v3.1 Base Score	6.6
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H</a>
CWE	CWE-416: Use After Free

**Vulnerability CVE-2024-43834**

In the Linux kernel, the following vulnerability has been resolved:

xdp: fix invalid wait context of page\_pool\_destroy()

If the driver uses a page pool, it creates a page pool with page\_pool\_create(). The reference count of page pool is 1 as default. A page pool will be destroyed only when a reference count reaches 0. page\_pool\_destroy() is used to destroy page pool, it decreases a reference count. When a page pool is destroyed, ->disconnect() is called, which is mem\_allocator\_disconnect(). This function internally acquires mutex\_lock().

If the driver uses XDP, it registers a memory model with xdp\_rxq\_info\_reg\_mem\_model(). The xdp\_rxq\_info\_reg\_mem\_model() internally increases a page pool reference count if a memory model is a page pool. Now the reference count is 2.

To destroy a page pool, the driver should call both page\_pool\_destroy() and xdp\_unreg\_mem\_model(). The xdp\_unreg\_mem\_model() internally calls page\_pool\_destroy(). Only page\_pool\_destroy() decreases a reference count.

If a driver calls page\_pool\_destroy() then xdp\_unreg\_mem\_model(), we will face an invalid wait context warning. Because xdp\_unreg\_mem\_model() calls page\_pool\_destroy() with rcu\_read\_lock(). The page\_pool\_destroy() internally acquires mutex\_lock().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

**Vulnerability CVE-2024-43856**

In the Linux kernel, the following vulnerability has been resolved:

dma: fix call order in dmam\_free\_coherent

dmam\_free\_coherent() frees a DMA allocation, which makes the freed vaddr available for reuse, then calls devres\_destroy() to remove and free the data structure used to track the DMA allocation. Between the two calls, it is possible for a concurrent task to make an allocation with the same vaddr and add it to the devres list.

If this happens, there will be two entries in the devres list with the same vaddr and devres\_destroy() can free the wrong entry, triggering the WARN\_ON() in dmam\_match.

Fix by destroying the devres entry before freeing the DMA allocation.

kokonut //net/encryption <http://sponge2/b9145fe6-0f72-4325-ac2f-a84d81075b03>

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

**Vulnerability CVE-2024-43858**

In the Linux kernel, the following vulnerability has been resolved:

jfs: Fix array-index-out-of-bounds in diFree

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-129: Improper Validation of Array Index

### **Vulnerability CVE-2024-43871**

In the Linux kernel, the following vulnerability has been resolved: devres: Fix memory leakage caused by driver API devm\_free\_percpu() It will cause memory leakage when use driver API devm\_free\_percpu() to free memory allocated by devm\_alloc\_percpu(), fixed by using devres\_release() instead of devres\_destroy() within devm\_free\_percpu().

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-416: Use After Free

### **Vulnerability CVE-2024-43879**

wifi: cfg80211: Currently NL80211\_RATE\_INFO\_HE\_RU\_ALLOC\_2x996 is not handled in cfg80211\_calculate\_bitrate\_he(), leading to warning.

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-20: Improper Input Validation

### **Vulnerability CVE-2024-43882**

exec: the execution may gain unintended 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](#)  
CWE CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-43889**

padata: vulnerability due to a possible divide-by-zero error in padata\_mt\_helper() during bootup, caused by an uninitialized chunk\_size being zero.

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-20: Improper Input Validation

### **Vulnerability CVE-2024-43890**

tracing: vulnerability due to an overflow in get\_free\_elt(), which could lead to infinite loops and CPU hangs when the tracing map becomes full.

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-20: Improper Input Validation

### **Vulnerability CVE-2024-43893**

serial: core: vulnerability due to a missing check for uartclk being zero, leading to a potential divide-by-zero error when calling ioctl TIOCSSERIAL with an invalid baud\_base.

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-20: Improper Input Validation

**Vulnerability CVE-2024-44935**

sctp: Fix null-ptr-deref in reuseport\_add\_sock(). A Null Pointer Dereference in reuseport\_add\_sock() while accessing sk2->sk\_reuseport\_cb. The repro first creates a listener with SO\_REUSEPORT. Then, it creates another listener on the same port and concurrently closes the first listener. The second listen() calls reuseport\_add\_sock() with the first listener as sk2, where sk2->sk\_reuseport\_cb is not expected to be cleared concurrently, but the close() does clear it by reuseport\_detach\_sock().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-44944**

In the Linux kernel, the following vulnerability has been resolved: netfilter: ctnetlink: use helper function to calculate expect ID Delete expectation path is missing a call to the nf\_expect\_get\_id() helper function to calculate the expectation ID, otherwise LSB of the expectation object address is leaked to userspace.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-401: Missing Release of Memory after Effective Lifetime

**Vulnerability CVE-2024-44948**

In the Linux kernel, the following vulnerability has been resolved:

x86/mtrr: Check if fixed MTRRs exist before saving them

MTRRs have an obsolete fixed variant for fine grained caching control of the 640K-1MB region that uses separate MSR. This fixed variant has a separate capability bit in the MTRR capability MSR.

So far all x86 CPUs which support MTRR have this separate bit set, so it went unnoticed that mtrr\_save\_state() does not check the capability bit before accessing the fixed MTRR MSRs.

Though on a CPU that does not support the fixed MTRR capability this results in a #GP. The #GP itself is harmless because the RDMSR fault is handled gracefully, but results in a WARN\_ON().

Add the missing capability check to prevent this.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

**Vulnerability CVE-2024-44960**

usb: gadget: core: Check for unset descriptor. It needs to be reassured that the descriptor has been set before looking at maxpacket. This fixes a null pointer panic in this case. This may happen if the gadget doesn't properly set up the endpoint for the current speed, or the gadget descriptors are malformed and the descriptor for the speed/endpoint are not found. No current gadget driver is known to have this problem, but this may cause a hard-to-find bug during development of new gadgets.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

**Vulnerability CVE-2024-44987**

In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent UAF in ip6\_send\_skb().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2024-44989**

In the Linux kernel, the following vulnerability has been resolved: bonding: fix xfrm real\_dev 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](#)  
CWE CWE-476: NULL Pointer Dereference

### **Vulnerability CVE-2024-44990**

In the Linux kernel, the following vulnerability has been resolved: bonding: fix null pointer deref in bond\_ipsec\_offload\_ok We must check if there is an active slave before dereferencing the pointer.

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-2024-45016**

In the Linux kernel, the following vulnerability has been resolved: netem: fix return value if duplicate enqueue fails.

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-416: Use After Free

### **Vulnerability CVE-2024-45018**

In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: initialise extack before use Fix missing initialisation of extack in flow offload.

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-456: Missing Initialization of a Variable

### **Vulnerability CVE-2024-46679**

In the Linux kernel, the following vulnerability has been resolved: ethtool: check device is present when getting link settings.

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-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-46743**

In the Linux kernel, the following vulnerability has been resolved: of/irq: Prevent device address out-of-bounds read in interrupt map walk.

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](#)  
CWE CWE-125: Out-of-bounds Read

### **Vulnerability CVE-2024-46744**

In the Linux kernel, the following vulnerability has been resolved: Squashfs: sanity check symbolic link size.

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-908: Use of Uninitialized Resource

**Vulnerability CVE-2024-46745**

In the Linux kernel, the following vulnerability has been resolved: Input: uinput - reject requests with unreasonable number of slots When exercising uinput interface syzkaller may try setting up device with a really large number of slots, which causes memory allocation failure in `input_mt_init_slots()`. While this allocation failure is handled properly and request is rejected, it results in syzkaller reports. Additionally, such request may put undue burden on the system which will try to free a lot of memory for a bogus request. Fix it by limiting allowed number of slots to 100. This can easily be extended if we see devices that can track more than 100 contacts.

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](#)  
CWE CWE-400: Uncontrolled Resource Consumption

**Vulnerability CVE-2024-46750**

In the Linux kernel, the following vulnerability has been resolved: PCI: Add missing bridge lock to `pci_bus_lock()`.

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-413: Improper Resource Locking

**Vulnerability CVE-2024-46759**

In the Linux kernel, the following vulnerability has been resolved: hwmon: (adc128d818) Fix underflows seen when writing limit attributes `DIV_ROUND_CLOSEST()` after `kstrtol()` results in an underflow if a large negative number such as -9223372036854775808 is provided by the user. Fix it by reordering `clamp_val()` and `DIV_ROUND_CLOSEST()` operations.

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-124: Buffer Underwrite ('Buffer Underflow')

**Vulnerability CVE-2024-46783**

In the Linux kernel, the following vulnerability has been resolved: tcp\_bpf: fix return value of `tcp_bpf_sendmsg()`.

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-229: Improper Handling of Values

**Vulnerability CVE-2024-46854**

In the Linux kernel, the following vulnerability has been resolved:

net: dpaa: Pad packets to `ETH_ZLEN`

When sending packets under 60 bytes, up to three bytes of the buffer following the data may be leaked. Avoid this by extending all packets to `ETH_ZLEN`, ensuring nothing is leaked in the padding. This bug can be reproduced by running

```
\lstinline|$ ping -s 11 destination
```

|  
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](#)  
CWE CWE-125: Out-of-bounds Read

### **Vulnerability CVE-2024-46865**

In the Linux kernel, the following vulnerability has been resolved:

fou: fix initialization of grc The grc must be initialize first. There can be a condition where if fou is NULL, goto out will be executed and grc would be used uninitialized.

CVSS v3.1 Base Score	7.1
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H</a>
CWE	CWE-908: Use of Uninitialized Resource

### **Vulnerability CVE-2024-47660**

In the Linux kernel, the following vulnerability has been resolved: fsnotify: clear PARENT\_WATCHED flags lazily In some setups directories can have many (usually negative) dentries. Hence \_\_fsnotify\_update\_child\_dentry\_flags() function can take a significant amount of time. Since the bulk of this function happens under inode->i\_lock this causes a significant contention on the lock when we remove the watch from the directory as the \_\_fsnotify\_update\_child\_dentry\_flags() call from fsnotify\_recalc\_mask() races with \_\_fsnotify\_update\_child\_dentry\_flags() calls from \_\_fsnotify\_parent() happening on children. This can lead upto softlockup reports reported by users. Fix the problem by calling fsnotify\_update\_children\_dentry\_flags() to set PARENT\_WATCHED flags only when parent starts watching children. When parent stops watching children, clear false positive PARENT\_WATCHED flags lazily in \_\_fsnotify\_parent() for each accessed child.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-413: Improper Resource Locking

### **Vulnerability CVE-2024-47672**

In the Linux kernel, the following vulnerability has been resolved:

wifi: iwlfwifi: mvm: don't wait for tx queues if firmware is dead

There is a WARNING in iwlfwifi\_trans\_wait\_tx\_queues\_empty() (that was recently converted from just a message), that can be hit if we wait for TX queues to become empty after firmware died. Clearly, we can't expect anything from the firmware after it's declared dead.

Don't call iwlfwifi\_trans\_wait\_tx\_queues\_empty() in this case. While it could be a good idea to stop the flow earlier, the flush functions do some maintenance work that is not related to the firmware, so keep that part of the code running even when the firmware is not running.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

**Vulnerability CVE-2024-47684**

In the Linux kernel, the following vulnerability has been resolved:

tcp: check skb is non-NULL in tcp\_rto\_delta\_us()

We have some machines running stock Ubuntu 20.04.6 which is their 5.4.0-174-generic kernel that are running ceph and recently hit a null ptr dereference in tcp\_rearm\_rto(). Initially hitting it from the TLP path, but then later we also saw it getting hit from the RACK case as well. Here are examples of the oops messages we saw in each of those cases:

```
Jul 26 15:05:02 rx [11061395.780353] BUG: kernel NULL pointer dereference, address:
0000000000000020 Jul 26 15:05:02 rx [11061395.787572] #PF: supervisor read access in
kernel mode Jul 26 15:05:02 rx [11061395.792971] #PF: error_code(0x0000) - not-present page Jul
26 15:05:02 rx [11061395.798362] PGD 0 P4D 0 Jul 26 15:05:02 rx [11061395.801164] Oops: 0000
[#1] SMP NOPTI Jul 26 15:05:02 rx [11061395.805091] CPU: 0 PID: 9180 Comm: msgr-worker-1
Tainted: G W 5.4.0-174-generic #193-Ubuntu Jul 26 15:05:02 rx [11061395.814996] Hardware name:
Supermicro SMC 2x26 os-gen8 64C NVME-Y 256G/H12SSW-NTR, BIOS 2.5.V1.2U.NVMe.UEFI
05/09/2023 Jul 26 15:05:02 rx [11061395.825952] RIP: 0010:tcp_rearm_rto+0xe4/0x160 Jul 26
15:05:02 rx [11061395.830656] Code: 87 ca 04 00 00 00 5b 41 5c 41 5d 5d c3 c3 49 8b bc
24 40 06 00 00 eb 8d 48 bb cf f7 53 e3 a5 9b c4 20 4c 89 ef e8 0c fe 0e 00 <48> 8b 78 20
48 c1 ef 03 48 89 f8 41 8b bc 24 80 04 00 00 48 f7 e3 Jul 26 15:05:02 rx [11061395.849665]
RSP: 0018:ffffb75d40003e08 EFLAGS: 00010246 Jul 26 15:05:02 rx [11061395.855149] RAX:
0000000000000000 RBX: 20c49ba5e353f7cf RCX: 0000000000000000 Jul 26 15:05:02 rx
[11061395.862542] RDX: 0000000062177c30 RSI: 000000000000231c RDI: ffff9874ad283a60
Jul 26 15:05:02 rx [11061395.869933] RBP: ffff75d40003e20 R08: 0000000000000000
R09: ffff987605e20aa8 Jul 26 15:05:02 rx [11061395.877318] R10: ffff75d40003f00 R11:
ffffb75d4460f740 R12: ffff9874ad283900 Jul 26 15:05:02 rx [11061395.884710] R13: ffff9874ad283a60
R14: ffff9874ad283980 R15: ffff9874ad283d30 Jul 26 15:05:02 rx [11061395.892095] FS:
00007f1ef4a2e700(0000) GS:ffff987605e00000(0000) knlGS:0000000000000000 Jul 26 15:05:02
rx [11061395.900438] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 Jul 26 15:05:02 rx
[11061395.906435] CR2: 0000000000000020 CR3: 0000003e450ba003 CR4: 000000000760ef0
Jul 26 15:05:02 rx [11061395.913822] PKRU: 55555554 Jul 26 15:05:02 rx [11061395.916786]
Call Trace: Jul 26 15:05:02 rx [11061395.919488] Jul 26 15:05:02 rx [11061395.921765] ?
show_regs.cold+0x1a/0x1f Jul 26 15:05:02 rx [11061395.925859] ? __die+0x90/0xd9 Jul 26
15:05:02 rx [11061395.929169] ? no_context+0x196/0x380 Jul 26 15:05:02 rx [11061395.933088] ?
ip6_protocol_deliver_rcu+0x4e0/0x4e0 Jul 26 15:05:02 rx [11061395.938216] ? ip6_sublist_rcv_finish+0x3d/0x50
Jul 26 15:05:02 rx [11061395.943000] ? __bad_area_nosemaphore+0x50/0x1a0 Jul 26 15:05:02 rx
[11061395.947873] ? bad_area_nosemaphore+0x16/0x20 Jul 26 15:05:02 rx [11061395.952486] ?
do_user_addr_fault+0x267/0x450 Jul 26 15:05:02 rx [11061395.957104] ? ipv6_list_rcv+0x112/0x140
Jul 26 15:05:02 rx [11061395.961279] ? __do_page_fault+0x58/0x90 Jul 26 15:05:02 rx
[11061395.965458] ? do_page_fault+0x2c/0xe0 Jul 26 15:05:02 rx [11061395.969465] ?
page_fault+0x34/0x40 Jul 26 15:05:02 rx [11061395.973217] ? tcp_rearm_rto+0xe4/0x160
Jul 26 15:05:02 rx [11061395.977313] ? tcp_rearm_rto+0xe4/0x160 Jul 26 15:05:02 rx
[11061395.981408] tcp_send_loss_probe+0x10b/0x220 Jul 26 15:05:02 rx [11061395.985937]
tcp_write_timer_handler+0x1b4/0x240 Jul 26 15:05:02 rx [11061395.990809] tcp_write_timer+0x9e/0xe0
Jul 26 15:05:02 rx [11061395.994814] ? tcp_write_timer_handler+0x240/0x240 Jul 26 15:05:02 rx
[11061395.999866] call_timer_fn+0x32/0x130 Jul 26 15:05:02 rx [11061396.003782] __run_timers.part.0+0x180/0x280
Jul 26 15:05:02 rx [11061396.008309] ? recalibrate_cpu_khz+0x10/0x10 Jul 26 15:05:02 rx
[11061396.012841] ? native_x2apic_icr_write+0x30/0x30 Jul 26 15:05:02 rx [11061396.017718] ?
lapic_next_even—truncated—
```

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-47685**

In the Linux kernel, the following vulnerability has been resolved:

netfilter: nf\_reject\_ipv6: fix nf\_reject\_ip6\_tcphdr\_put()

syzbot reported that nf\_reject\_ip6\_tcphdr\_put() was possibly sending garbage on the four reserved tcp bits (th->res1)

Use skb\_put\_zero() to clear the whole TCP header, as done in nf\_reject\_ip\_tcphdr\_put()

BUG: KMSAN: uninit-value in nf\_reject\_ip6\_tcphdr\_put+0x688/0x6c0 net/ipv6/netfilter/nf\_reject\_ipv6.c:255  
 nf\_reject\_ip6\_tcphdr\_put+0x688/0x6c0 net/ipv6/netfilter/nf\_reject\_ipv6.c:255 nf\_send\_reset6+0xd84/0x15b0  
 net/ipv6/netfilter/nf\_reject\_ipv6.c:344 nft\_reject\_inet\_eval+0x3c1/0x880 net/netfilter/nft\_reject\_inet.c:48  
 expr\_call\_ops\_eval net/netfilter/nf\_tables\_core.c:240 [inline] nft\_do\_chain+0x438/0x22a0 net/net-  
 filter/nf\_tables\_core.c:288 nft\_do\_chain\_inet+0x41a/0x4f0 net/netfilter/nft\_chain\_filter.c:161  
 nf\_hook\_entry\_hookfn include/linux/netfilter.h:154 [inline] nf\_hook\_slow+0xf4/0x400 net/netfil-  
 ter/core.c:626 nf\_hook include/linux/netfilter.h:269 [inline] NF\_HOOK include/linux/netfilter.h:312 [inline]  
 ipv6\_rcv+0x29b/0x390 net/ipv6/ip6\_input.c:310 \_\_netif\_receive\_skb\_one\_core net/core/dev.c:5661  
 [inline] \_\_netif\_receive\_skb+0x1da/0xa00 net/core/dev.c:5775 process\_backlog+0x4ad/0xa50 net/-  
 core/dev.c:6108 \_\_napi\_poll+0xe7/0x980 net/core/dev.c:6772 napi\_poll net/core/dev.c:6841 [inline]  
 net\_rx\_action+0xa5a/0x19b0 net/core/dev.c:6963 handle\_softirqs+0x1ce/0x800 kernel/softirq.c:554  
 \_\_do\_softirq+0x14/0x1a kernel/softirq.c:588 do\_softirq+0x9a/0x100 kernel/softirq.c:455 \_\_lo-  
 cal\_bh\_enable\_ip+0x9f/0xb0 kernel/softirq.c:382 local\_bh\_enable include/linux/bottom\_half.h:33 [inline]  
 rcu\_read\_unlock\_bh include/linux/rcupdate.h:908 [inline] \_\_dev\_queue\_xmit+0x2692/0x5610 net/-  
 core/dev.c:4450 dev\_queue\_xmit include/linux/netdevice.h:3105 [inline] neigh\_resolve\_output+0x9ca/0xae0  
 net/core/neighbour.c:1565 neigh\_output include/net/neighbour.h:542 [inline] ip6\_finish\_output2+0x2347/0x2ba0  
 net/ipv6/ip6\_output.c:141 \_\_ip6\_finish\_output net/ipv6/ip6\_output.c:215 [inline] ip6\_finish\_output+0xbb8/0x14b0  
 net/ipv6/ip6\_output.c:226 NF\_HOOK\_COND include/linux/netfilter.h:303 [inline] ip6\_output+0x356/0x620  
 net/ipv6/ip6\_output.c:247 dst\_output include/net/dst.h:450 [inline] NF\_HOOK include/linux/netfil-  
 ter.h:314 [inline] ip6\_xmit+0x1ba6/0x25d0 net/ipv6/ip6\_output.c:366 inet6\_csk\_xmit+0x442/0x530  
 net/ipv6/inet6\_connection\_sock.c:135 \_\_tcp\_transmit\_skb+0x3b07/0x4880 net/ipv4/tcp\_output.c:1466  
 tcp\_transmit\_skb net/ipv4/tcp\_output.c:1484 [inline] tcp\_connect+0x35b6/0x7130 net/ipv4/tcp\_output.c:4143  
 tcp\_v6\_connect+0x1bcc/0x1e40 net/ipv6/tcp\_ipv6.c:333 \_\_inet\_stream\_connect+0x2ef/0x1730  
 net/ipv4/af\_inet.c:679 inet\_stream\_connect+0x6a/0xd0 net/ipv4/af\_inet.c:750 \_\_sys\_connect\_file  
 net/socket.c:2061 [inline] \_\_sys\_connect+0x606/0x690 net/socket.c:2078 \_\_do\_sys\_connect net/-  
 socket.c:2088 [inline] \_\_se\_sys\_connect net/socket.c:2085 [inline] \_\_x64\_sys\_connect+0x91/0xe0  
 net/socket.c:2085 x64\_sys\_call+0x27a5/0x3ba0 arch/x86/include/generated/asm/syscalls\_64.h:43  
 do\_syscall\_x64 arch/x86/entry/common.c:52 [inline] do\_syscall\_64+0xcd/0x1e0 arch/x86/entry/common.c:83  
 entry\_SYSCALL\_64\_after\_hwframe+0x77/0x7f

Uninit was stored to memory at: nf\_reject\_ip6\_tcphdr\_put+0x60c/0x6c0 net/ipv6/netfilter/nf\_reject\_ipv6.c:249  
 nf\_send\_reset6+0xd84/0x15b0 net/ipv6/netfilter/nf\_reject\_ipv6.c:344 nft\_reject\_inet\_eval+0x3c1/0x880  
 net/netfilter/nft\_reject\_inet.c:48 expr\_call\_ops\_eval net/netfilter/nf\_tables\_core.c:240 [inline]  
 nft\_do\_chain+0x438/0x22a0 net/netfilter/nf\_tables\_core.c:288 nft\_do\_chain\_inet+0x41a/0x4f0  
 net/netfilter/nft\_chain\_filter.c:161 nf\_hook\_entry\_hookfn include/linux/netfilter.h:154 [inline]  
 nf\_hook\_slow+0xf4/0x400 net/netfilter/core.c:626 nf\_hook include/linux/netfilter.h:269 [inline]  
 NF\_HOOK include/linux/netfilter.h:312 [inline] ipv6\_rcv+0x29b/0x390 net/ipv6/ip6\_input.c:310  
 \_\_netif\_receive\_skb\_one\_core —truncated—

CVSS v3.1 Base Score	9.1
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H</a>
CWE	CWE-908: Use of Uninitialized Resource

**Vulnerability CVE-2024-47692**

In the Linux kernel, the following vulnerability has been resolved:

nfsd: return -EINVAL when namelen is 0 When we have a corrupted main.sqlite in /var/lib/nfs/nfsdclid/, it may result in namelen being 0, which will cause memdup\_user() to return ZERO\_SIZE\_PTR. When we access the name.data that has been assigned the value of ZERO\_SIZE\_PTR in nfs4\_client\_to\_reclaim(), null pointer dereference is triggered.

```
[ T1205] ===== [
T1205] BUG: KASAN: null-ptr-deref in nfs4_client_to_reclaim+0xe9/0x260 [ T1205] Read of size 1 at
addr 0000000000000010 by task nfsdclid/1205 [ T1205] [ T1205] CPU: 11 PID: 1205 Comm: nfsdclid
Not tainted 5.10.0-00003-g2c1423731b8d #406 [ T1205] Hardware name: QEMU Standard PC (i440FX
+ PIIX, 1996), BIOS ?-20190727_073836-buildvm-ppc64le-16.ppc.fedoraproject.org-3.fc31 04/01/2014
[ T1205] Call Trace: [ T1205] dump_stack+0x9a/0xd0 [ T1205] ? nfs4_client_to_reclaim+0xe9/0x260
[ T1205] __kasan_report.cold+0x34/0x84 [ T1205] ? nfs4_client_to_reclaim+0xe9/0x260 [
T1205] kasan_report+0x3a/0x50 [ T1205] nfs4_client_to_reclaim+0xe9/0x260 [ T1205] ?
nfsd4_release_lockowner+0x410/0x410 [ T1205] cld_pipe_downcall+0x5ca/0x760 [ T1205] ?
nfsd4_cld_tracking_exit+0x1d0/0x1d0 [ T1205] ? down_write_killable_nested+0x170/0x170 [
T1205] ? avc_policy_seqno+0x28/0x40 [ T1205] ? selinux_file_permission+0x1b4/0x1e0 [ T1205]
rpc_pipe_write+0x84/0xb0 [ T1205] vfs_write+0x143/0x520 [ T1205] ksys_write+0xc9/0x170 [
T1205] ? __ia32_sys_read+0x50/0x50 [ T1205] ? ktime_get_coarse_real_ts64+0xfe/0x110 [
T1205] ? ktime_get_coarse_real_ts64+0xa2/0x110 [ T1205] do_syscall_64+0x33/0x40 [ T1205]
entry_SYSCALL_64_after_hwframe+0x67/0xd1 [ T1205] RIP: 0033:0x7fdbdb761bc7 [ T1205] Code:
0f 00 f7 d8 64 89 02 48 c7 c0 ff ff ff ff eb b7 0f 1f 00 f3 0f 1e fa 64 8b 04 25 18 00 00 00 85 c0 75
10 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 514 [ T1205] RSP: 002b:00007fff8c4b7248 EFLAGS:
00000246 ORIG_RAX: 0000000000000001 [ T1205] RAX: ffffffffda RBX: 000000000000042b RCX:
00007fdbdb761bc7 [ T1205] RDX: 000000000000042b RSI: 00007fff8c4b75f0 RDI: 0000000000000008
[ T1205] RBP: 00007fdbdb761bb0 R08: 0000000000000000 R09: 0000000000000001 [
T1205] R10: 0000000000000000 R11: 0000000000000246 R12: 000000000000042b [
T1205] R13: 0000000000000008 R14: 00007fff8c4b75f0 R15: 0000000000000000 [ T1205]
=====
```

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
CWE	CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-47696**

In the Linux kernel, the following vulnerability has been resolved:

RDMA/iwcm: Fix WARNING:at\_kernel/workqueue.c:#check\_flush\_dependency

In the commit aee2424246f9 ("RDMA/iwcm: Fix a use-after-free related to destroying CM IDs"), the function flush\_workqueue is invoked to flush the work queue iwcm\_wq.

But at that time, the work queue iwcm\_wq was created via the function alloc\_ordered\_workqueue without the flag WQ\_MEM\_RECLAIM.

Because the current process is trying to flush the whole iwcm\_wq, if iwcm\_wq doesn't have the flag WQ\_MEM\_RECLAIM, verify that the current process is not reclaiming memory or running on a workqueue which doesn't have the flag WQ\_MEM\_RECLAIM as that can break forward-progress guarantee leading to a deadlock.

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-2024-47697**

In the Linux kernel, the following vulnerability has been resolved:

drivers: media: dvb-frontends/rtl2830: fix an out-of-bounds write error

Ensure index in rtl2830\_pid\_filter does not exceed 31 to prevent out-of-bounds access.

dev->filters is a 32-bit value, so set\_bit and clear\_bit functions should only operate on indices from 0 to 31. If index is 32, it will attempt to access a non-existent 33rd bit, leading to out-of-bounds access. Change the boundary check from index > 32 to index >= 32 to resolve this issue.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-787: Out-of-bounds Write

### **Vulnerability CVE-2024-47699**

In the Linux kernel, the following vulnerability has been resolved:

nilfs2: fix potential null-ptr-deref in nilfs\_btree\_insert()

Patch series “nilfs2: fix potential issues with empty b-tree nodes”.

This series addresses three potential issues with empty b-tree nodes that can occur with corrupted filesystem images, including one recently discovered by syzbot.

This patch (of 3):

If a b-tree is broken on the device, and the b-tree height is greater than 2 (the level of the root node is greater than 1) even if the number of child nodes of the b-tree root is 0, a NULL pointer dereference occurs in nilfs\_btree\_prepare\_insert(), which is called from nilfs\_btree\_insert().

This is because, when the number of child nodes of the b-tree root is 0, nilfs\_btree\_do\_lookup() does not set the block buffer head in any of path[x].bp\_bh, leaving it as the initial value of NULL, but if the level of the b-tree root node is greater than 1, nilfs\_btree\_get\_nonroot\_node(), which accesses the buffer memory of path[x].bp\_bh, is called.

Fix this issue by adding a check to nilfs\_btree\_root\_broken(), which performs sanity checks when reading the root node from the device, to detect this inconsistency.

Thanks to Lizhi Xu for trying to solve the bug and clarifying the cause early on.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

### **Vulnerability CVE-2024-47701**

In the Linux kernel, the following vulnerability has been resolved: ext4: avoid OOB when system.data xattr changes underneath the filesystem.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2024-47705**

In the Linux kernel, the following vulnerability has been resolved:

block: fix potential invalid pointer dereference in blk\_add\_partition

The blk\_add\_partition() function initially used a single if-condition (IS\_ERR(part)) to check for errors when adding a partition. This was modified to handle the specific case of -ENXIO separately, allowing the function to proceed without logging the error in this case. However, this change unintentionally left a path where md\_autodetect\_dev() could be called without confirming that part is a valid pointer.

This commit separates the error handling logic by splitting the initial if-condition, improving code readability and handling specific error scenarios explicitly. The function now distinguishes the general error case from -ENXIO without altering the existing behavior of md\_autodetect\_dev() calls.

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-2024-47706**

In the Linux kernel, the following vulnerability has been resolved:

block, bfq: fix possible UAF for bfqq->bic with merge chain

In this case, IO from Process 1 will get bfqq2 from BIC1 first, and then get bfqq3 through merge chain, and finally handle IO by bfqq3. However, current code will think bfqq2 is owned by BIC1, like initial state, and set bfqq2->bic to BIC1.

Allocated by task 20776: kasan\_save\_stack+0x20/0x40 mm/kasan/common.c:45 kasan\_set\_track+0x25/0x30 mm/kasan/common.c:52 \_\_kasan\_slab\_alloc+0x87/0x90 mm/kasan/common.c:328 kasan\_slab\_alloc include/linux/kasan.h:188 [inline] slab\_post\_alloc\_hook mm/slab.h:763 [inline] slab\_alloc\_node mm/slub.c:3458 [inline] kmem\_cache\_alloc\_node+0x1a4/0x6f0 mm/slub.c:3503 ioc\_create\_icq block/blk-ioc.c:370 [inline] —truncated—

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-416: Use After Free

### **Vulnerability CVE-2024-47707**

ipv6: A NULL dereference vulnerability may occur in rt6\_uncached\_list\_flush\_dev() due to the necessary check being removed by a previous commit.

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-2024-47709**

can: bcm: A warning is triggered when connect() is issued again for a socket whose connect()ed device has been unregistered. However, if the socket is just close()d without the 2nd connect(), the remaining bo->bcm\_proc\_read triggers unnecessary remove\_proc\_entry() in bcm\_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
CWE	CWE-825: Expired Pointer Dereference

### **Vulnerability CVE-2024-47710**

sock\_map: vulnerability result of adding a cond\_resched() in sock\_hash\_free() to prevent CPU soft lockups when destroying maps with a large number of buckets.

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-400: Uncontrolled Resource Consumption

### **Vulnerability CVE-2024-47713**

wifi: mac80211: vulnerability caused by implementing a two-phase skb reclamation in ieee80211\_do\_stop() to avoid warnings and potential issues caused by calling \_\_dev\_queue\_xmit() with interrupts disabled.

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-664: Improper Control of a Resource Through its Lifetime

### **Vulnerability CVE-2024-47718**

wifi: rtw88: vulnerability may lead to a use-after-free (UAF) error if firmware loading is not properly synchronized during USB initialization and disconnection.

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-416: Use After Free

### **Vulnerability CVE-2024-47723**

In the Linux kernel, the following vulnerability has been resolved:

jfs: fix out-of-bounds in dbNextAG() and diAlloc()

In dbNextAG(), there is no check for the case where bmp->db\_numag is greater or same than MAXAG due to a polluted image, which causes an out-of-bounds. Therefore, a bounds check should be added in dbMount().

And in dbNextAG(), a check for the case where agpref is greater than bmp->db\_numag should be added, so an out-of-bounds exception should be prevented.

Additionally, a check for the case where agno is greater or same than MAXAG should be added in diAlloc() to prevent out-of-bounds.

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](#)  
CWE CWE-125: Out-of-bounds Read

### **Vulnerability CVE-2024-47735**

RDMA/hns: misuse of spin\_lock\_irq()/spin\_unlock\_irq() when spin\_lock\_irqsave()/spin\_lock\_irqrestore() was hold.

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-667: Improper Locking

### **Vulnerability CVE-2024-47737**

In the Linux kernel, the following vulnerability has been resolved: nfsd: call cache\_put if xdr\_reserve\_space returns NULL.

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-2024-47747**

net: seq: Fix use after free vulnerability in ether3 Driver Due to Race Condition. In the ether3\_probe function, a timer is initialized with a callback function ether3\_ledoff, bound to &prev(dev)->timer. Once the timer is started, there is a risk of a race condition if the module or device is removed, triggering the ether3\_remove function to perform cleanup.

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-416: Use After Free

**Vulnerability CVE-2024-49851**

tpm: Clean up TPM space after command failure tpm\_dev\_transmit prepares the TPM space before attempting command transmission. However if the command fails no rollback of this preparation is done. This can result in transient handles being leaked if the device is subsequently closed with no further commands performed.

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-459: Incomplete Cleanup

**Vulnerability CVE-2024-49889**

In the Linux kernel, the following vulnerability has been resolved:

ext4: avoid use-after-free in ext4\_ext\_show\_leaf()

In ext4\_find\_extent(), path may be freed by error or be reallocated, so using a previously saved \*ppath may have been freed and thus may trigger use-after-free, as follows:

```
ext4_split_extent path = *ppath; ext4_split_extent_at(ppath) path = ext4_find_extent(ppath)
ext4_split_extent_at(ppath) // ext4_find_extent fails to free path // but zeroout succeeds
ext4_ext_show_leaf(inode, path) eh = path[depth].p_hdr // path use-after-free !!!
```

Similar to ext4\_split\_extent\_at(), we use \*ppath directly as an input to ext4\_ext\_show\_leaf(). Fix a spelling error by the way.

Same problem in ext4\_ext\_handle\_unwritten\_extents(). Since 'path' is only used in ext4\_ext\_show\_leaf(), remove 'path' and use \*ppath directly.

This issue is triggered only when EXT\_DEBUG is defined and therefore does not affect functionality.

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-2024-49890**

In the Linux kernel, the following vulnerability has been resolved:

drm/amd/pm: ensure the fw\_info is not null before using it

This resolves the dereference null return value warning reported by Coverity.

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-2024-49892**

In the Linux kernel, the following vulnerability has been resolved:

drm/amd/display: Initialize get\_bytes\_per\_element's default to 1

Variables, used as denominators and maybe not assigned to other values, should not be 0. bytes\_per\_element\_y & bytes\_per\_element\_c are initialized by get\_bytes\_per\_element() which should never return 0.

This fixes 10 DIVIDE\_BY\_ZERO issues reported by Coverity.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-369: Divide By Zero

### **Vulnerability CVE-2024-49894**

In the Linux kernel, the following vulnerability has been resolved:

drm/amd/display: Fix index out of bounds in degamma hardware format translation

Fixes index out of bounds issue in `cm_helper_translate_curve_to_degamma_hw_format` function. The issue could occur when the index 'i' exceeds the number of transfer function points (TRANSFER\_FUNC\_POINTS).

The fix adds a check to ensure 'i' is within bounds before accessing the transfer function points. If 'i' is out of bounds the function returns false to indicate an error.

Reported by smatch: drivers/gpu/drm/amd/amdgpu/../display/dc/dcn10/dcn10\_cm\_common.c:594 cm\_helper\_translate\_curve\_to\_degamma\_hw\_format() error: buffer overflow 'output\_tf->tf\_pts.red' 1025 <= s32max drivers/gpu/drm/amd/amdgpu/../display/dc/dcn10/dcn10\_cm\_common.c:595 cm\_helper\_translate\_curve\_to\_degamma\_hw\_format() error: buffer overflow 'output\_tf->tf\_pts.green' 1025 <= s32max drivers/gpu/drm/amd/amdgpu/../display/dc/dcn10/dcn10\_cm\_common.c:596 cm\_helper\_translate\_curve\_to\_degamma\_hw\_format() error: buffer overflow 'output\_tf->tf\_pts.blue' 1025 <= s32max

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-129: Improper Validation of Array Index

### **Vulnerability CVE-2024-49900**

In the Linux kernel, the following vulnerability has been resolved:

jfs: Fix uninit-value access of new\_ea in ea\_buffer

syzbot reports that lzo1x\_1\_do\_compress is using uninit-value:

```
===== BUG: KMSAN: uninit-value in  
lzo1x_1_do_compress+0x19f9/0x2510 lib/lzo/lzo1x_compress.c:178
```

...

Uninit was stored to memory at: ea\_put fs/jfs/xattr.c:639 [inline]

...

Local variable ea\_buf created at: \_\_jfs\_setxattr+0x5d/0x1ae0 fs/jfs/xattr.c:662 \_\_jfs\_xattr\_set+0xe6/0x1f0 fs/jfs/xattr.c:934

```
=====
```

The reason is ea\_buf->new\_ea is not initialized properly.

Fix this by using memset to empty its content at the beginning in ea\_get().

CVSS v3.1 Base Score	7.1
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H</a>
CWE	CWE-908: Use of Uninitialized Resource

### **Vulnerability CVE-2024-49902**

jfs: vulnerability caused by assigning msm\_gpu->pdev earlier in the initialization process to prevent null pointer dereferences in msm\_gpu\_cleanup.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-125: Out-of-bounds Read

**Vulnerability CVE-2024-49903**

In the Linux kernel, the following vulnerability has been resolved:

jfs: Fix uaf in dbFreeBits

**[syzbot reported]**

BUG: KASAN: slab-use-after-free in \_\_mutex\_lock\_common kernel/locking/mutex.c:587 [inline] BUG: KASAN: slab-use-after-free in \_\_mutex\_lock+0xfe/0xd70 kernel/locking/mutex.c:752 Read of size 8 at addr ffff8880229254b0 by task syz-executor357/5216

CPU: 0 UID: 0 PID: 5216 Comm: syz-executor357 Not tainted 6.11.0-rc3-syzkaller-00156-gd7a5aa4b3c00 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024 Call Trace: <TASK> \_\_dump\_stack lib/dump\_stack.c:93 [inline] dump\_stack\_lvl+0x241/0x360 lib/dump\_stack.c:119 print\_address\_description mm/kasan/report.c:377 [inline] print\_report+0x169/0x550 mm/kasan/report.c:488 kasan\_report+0x143/0x180 mm/kasan/report.c:601 \_\_mutex\_lock\_common kernel/locking/mutex.c:587 [inline] \_\_mutex\_lock+0xfe/0xd70 kernel/locking/mutex.c:752 dbFreeBits+0x7ea/0xd90 fs/jfs/jfs\_dmap.c:2390 dbFreeDmap fs/jfs/jfs\_dmap.c:2089 [inline] dbFree+0x35b/0x680 fs/jfs/jfs\_dmap.c:409 dbDiscardAG+0x8a9/0xa20 fs/jfs/jfs\_dmap.c:1650 jfs\_ioc\_trim+0x433/0x670 fs/jfs/jfs\_discard.c:100 jfs\_ioctl+0x2d0/0x3e0 fs/jfs/jfs\_ioctl.c:131 vfs\_ioctl fs/ioctl.c:51 [inline] \_\_do\_sys\_ioctl fs/ioctl.c:907 [inline] \_\_se\_sys\_ioctl+0xfc/0x170 fs/ioctl.c:893 do\_syscall\_x64 arch/x86/entry/common.c:52 [inline] do\_syscall\_64+0xf3/0x230 arch/x86/entry/common.c:83

Freed by task 5218: kasan\_save\_stack mm/kasan/common.c:47 [inline] kasan\_save\_track+0x3f/0x80 mm/kasan/common.c:68 kasan\_save\_free\_info+0x40/0x50 mm/kasan/generic.c:579 poison\_slab\_object+0xe0/0x150 mm/kasan/common.c:240 \_\_kasan\_slab\_free+0x37/0x60 mm/kasan/common.c:256 kasan\_slab\_free include/linux/kasan.h:184 [inline] slab\_free\_hook mm/slub.c:2252 [inline] slab\_free mm/slub.c:4473 [inline] kfree+0x149/0x360 mm/slub.c:4594 dbUnmount+0x11d/0x190 fs/jfs/jfs\_dmap.c:278 jfs\_mount\_rw+0x4ac/0x6a0 fs/jfs/jfs\_mount.c:247 jfs\_remount+0x3d1/0x6b0 fs/jfs/super.c:454 reconfigure\_super+0x445/0x880 fs/super.c:1083 vfs\_cmd\_reconfigure fs/fsopen.c:263 [inline] vfs\_fsconfig\_locked fs/fsopen.c:292 [inline] \_\_do\_sys\_fsconfig fs/fsopen.c:473 [inline] \_\_se\_sys\_fsconfig+0xb6e/0xf80 fs/fsopen.c:345 do\_syscall\_x64 arch/x86/entry/common.c:52 [inline] do\_syscall\_64+0xf3/0x230 arch/x86/entry/common.c:83 entry\_SYSCALL\_64\_after\_hwframe+0x77/0x7f

[Analysis] There are two paths (dbUnmount and jfs\_ioc\_trim) that generate race condition when accessing bmap, which leads to the occurrence of uaf.

Use the lock s\_ument to synchronize them, in order to avoid uaf caused by race condition.

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-416: Use After Free

**Vulnerability CVE-2024-49930**

wifi: ath11k: fix array out-of-bound access in SoC stats. Currently, the ath11k\_soc\_dp\_stats::hal\_reo\_error array is defined with a maximum size of DP\_REO\_DST\_RING\_MAX. However, the ath11k\_dp\_process\_rx() function access ath11k\_soc\_dp\_stats::hal\_reo\_error using the REO destination SRNG ring ID, which is incorrect. SRNG ring ID differ from normal ring ID, and this usage leads to out-of-bounds array access.

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
CWE	CWE-125: Out-of-bounds Read

**Vulnerability CVE-2024-49938**

In the Linux kernel, the following vulnerability has been resolved:

wifi: ath9k\_htc: Use `__skb_set_length()` for resetting urb before resubmit

Syzbot points out that `skb_trim()` has a sanity check on the existing length of the `skb`, which can be uninitialised in some error paths. The intent here is clearly just to reset the length to zero before resubmitting, so switch to calling `__skb_set_length(skb, 0)` directly. In addition, `__skb_set_length()` already contains a call to `skb_reset_tail_pointer()`, so remove the redundant call.

The syzbot report came from `ath9k_hif_usb_reg_in_cb()`, but there's a similar usage of `skb_trim()` in `ath9k_hif_usb_rx_cb()`, change both while we're at it.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-824: Access of Uninitialized Pointer

**Vulnerability CVE-2024-49944**

sctp: set `sk_state` back to CLOSED if autobind fails in `sctp_listen_start`. In `sctp_listen_start()` invoked by `sctp_inet_listen()`, it should set the `sk_state` back to CLOSED if `sctp_autobind()` fails due to whatever reason. Otherwise, next time when calling `sctp_inet_listen()`, if `sctp_sk(sk)->reuse` is already set via `setsockopt(SCTP_REUSE_PORT)`, `sctp_sk(sk)->bind_hash` will be dereferenced as `sk_state` is LISTENING, which causes a crash as `bind_hash` is NULL

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-49948**

In the Linux kernel, the following vulnerability has been resolved: net: add more sanity checks to `qdisc_pkt_len_init()`.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-124: Buffer Underwrite ('Buffer Underflow')

**Vulnerability CVE-2024-49949**

In the Linux kernel, the following vulnerability has been resolved: net: avoid potential underflow in `qdisc_pkt_len_init()` with UFO.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-124: Buffer Underwrite ('Buffer Underflow')

**Vulnerability CVE-2024-49952**

In the Linux kernel, the following vulnerability has been resolved: netfilter: nf\_tables: prevent `nf_skb_duplicated` corruption.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-49955**

In the Linux kernel, the following vulnerability has been resolved:

ACPI: battery: Fix possible crash when unregistering a battery hook

When a battery hook returns an error when adding a new battery, then the battery hook is automatically unregistered. However the battery hook provider cannot know that, so it will later call `battery_hook_unregister()` on the already unregistered battery hook, resulting in a crash.

Fix this by using the list head to mark already unregistered battery hooks as already being unregistered so that they can be ignored by `battery_hook_unregister()`.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-672: Operation on a Resource after Expiration or Release

### **Vulnerability CVE-2024-49973**

r8169: RTL8125 added fields to the tally counter, this change could cause the chip to perform Direct Memory Access on these new fields, potentially writing to unallocated memory.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-787: Out-of-bounds Write

### **Vulnerability CVE-2024-49977**

net: stmmac: `port_transmit_rate_kbps` could be set to a value of 0, which is then passed to the “`div_s64`” function when `tc-cbs` is disabled. This leads to a zero-division error.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-49997**

In the Linux kernel, the following vulnerability has been resolved: `net: ethernet: lantiq_etop: fix memory disclosure` When applying padding, the buffer is not zeroed, which results in memory disclosure. The mentioned data is observed on the wire. This patch uses `skb_put_padto()` to pad Ethernet frames properly. The mentioned function zeroes the expanded buffer. In case the packet cannot be padded it is silently dropped. Statistics are also not incremented. This driver does not support statistics in the old 32-bit format or the new 64-bit format. These will be added in the future. In its current form, the patch should be easily backported to stable versions. Ethernet MACs on Amazon-SE and Danube cannot do padding of the packets in hardware, so software padding must be applied.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-226: Sensitive Information in Resource Not Removed Before Reuse

### **Vulnerability CVE-2024-50001**

In the Linux kernel, the following vulnerability has been resolved:

net/mlx5: Fix error path in multi-packet WQE transmit

Remove the erroneous unmap in case no DMA mapping was established

The multi-packet WQE transmit code attempts to obtain a DMA mapping for the skb. This could fail, e.g. under memory pressure, when the IOMMU driver just can't allocate more memory for page tables. While the code tries to handle this in the path below the `err_unmap` label it erroneously unmaps one entry from the sq's FIFO list of active mappings. Since the current map attempt failed this unmap is removing some random DMA mapping that might still be required. If the PCI function now presents that IOVA, the IOMMU may assume a rogue DMA access and e.g. on s390 puts the PCI function in error state.

The erroneous behavior was seen in a stress-test environment that created memory pressure.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-755: Improper Handling of Exceptional Conditions

### **Vulnerability CVE-2024-50006**

In the Linux kernel, the following vulnerability has been resolved: ext4: fix `i_data_sem` unlock order in `ext4_ind_migrate()`.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-833: Deadlock

### **Vulnerability CVE-2024-50008**

wifi: mwifiex: `memcpy()` field-spanning write warning in `mwifiex_cmd_802_11_scan_ext()` Replace one-element array with a flexible-array member in `struct host_cmd_ds_802_11_scan_ext`.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-787: Out-of-bounds Write

### **Vulnerability CVE-2024-50010**

In the Linux kernel, the following vulnerability has been resolved:

exec: don't WARN for racy path\_noexec check

Both `i_mode` and `noexec` checks wrapped in `WARN_ON` stem from an artifact of the previous implementation. They used to legitimately check for the condition, but that got moved up in two commits: 633fb6ac3980 ("exec: move `S_ISREG()` check earlier") 0fd338b2d2cd ("exec: move `path_noexec()` check earlier")

Instead of being removed said checks are `WARN_ON`'ed instead, which has some debug value.

However, the spurious `path_noexec` check is racy, resulting in unwarranted warnings should someone race with setting the `noexec` flag.

One can note there is more to perm-checking whether `execve` is allowed and none of the conditions are guaranteed to still hold after they were tested for.

Additionally this does not validate whether the code path did any perm checking to begin with – it will pass if the inode happens to be regular.

Keep the redundant `path_noexec()` check even though it's mindless nonsense checking for guarantee that isn't given so drop the `WARN`.

Reword the commentary and do small tidy ups while here.

[brauner: keep redundant `path_noexec()` check]

CVSS v3.1 Base Score	4.7
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-50015**

ext4: dax: Overflowing extents beyond inode size when partially writing.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-665: Improper Initialization

**Vulnerability CVE-2024-50033**

In the Linux kernel, the following vulnerability has been resolved:

slip: make slhc\_remember() more robust against malicious packets

syzbot found that slhc\_remember() was missing checks against malicious packets [1].

slhc\_remember() only checked the size of the packet was at least 20, which is not good enough.

We need to make sure the packet includes the IPv4 and TCP header that are supposed to be carried.

Add iph and th pointers to make the code more readable.

[1]

BUG: KMSAN: uninit-value in slhc\_remember+0x2e8/0x7b0 drivers/net/slip/slh.c:666 slhc\_remember+0x2e8/0x7b0 drivers/net/slip/slh.c:666 ppp\_receive\_nonmp\_frame+0xe45/0x35e0 drivers/net/ppp/ppp\_generic.c:2455 ppp\_receive\_frame drivers/net/ppp/ppp\_generic.c:2372 [inline] ppp\_do\_rcv+0x65f/0x40d0 drivers/net/ppp/ppp\_generic.c:2212 ppp\_input+0x7dc/0xe60 drivers/net/ppp/ppp\_generic.c:2327 pppoe\_rcv\_core+0x1d3/0x720 drivers/net/ppp/pppoe.c:379 sk\_backlog\_rcv+0x13b/0x420 include/net/socket.h:1113 \_\_release\_sock+0x1da/0x330 net/core/socket.c:3072 release\_sock+0x6b/0x250 net/core/socket.c:3626 pppoe\_sendmsg+0x2b8/0xb90 drivers/net/ppp/pppoe.c:903 sock\_sendmsg\_nosec net/socket.c:729 [inline] \_\_sock\_sendmsg+0x30f/0x380 net/socket.c:744 **sys\_sendmsg+0x903/0xb60 net/socket.c:2602** sys\_sendmsg+0x28d/0x3c0 net/socket.c:2656 \_\_sys\_sendmmsg+0x3c1/0x960 net/socket.c:2742 \_\_do\_sys\_sendmmsg net/socket.c:2771 [inline] \_\_se\_sys\_sendmmsg net/socket.c:2768 [inline] \_\_x64\_sys\_sendmmsg+0xbc/0x120 net/socket.c:2768 x64\_sys\_call+0xb6e/0x3ba0 arch/x86/include/generated/asm/syscalls\_64.h:308 do\_syscall\_x64 arch/x86/entry/common.c:52 [inline] do\_syscall\_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry\_SYSCALL\_64\_after\_hwframe+0x77/0x7f

Uninit was created at: slab\_post\_alloc\_hook mm/slub.c:4091 [inline] slab\_alloc\_node mm/slub.c:4134 [inline] kmem\_cache\_alloc\_node\_noprof+0x6bf/0xb80 mm/slub.c:4186 kmalloc\_reserve+0x13d/0x4a0 net/core/skbuff.c:587 \_\_alloc\_skb+0x363/0x7b0 net/core/skbuff.c:678 alloc\_skb include/linux/skbuff.h:1322 [inline] sock\_wmalloc+0xfe/0x1a0 net/core/socket.c:2732 pppoe\_sendmsg+0x3a7/0xb90 drivers/net/ppp/pppoe.c:867 sock\_sendmsg\_nosec net/socket.c:729 [inline] \_\_sock\_sendmsg+0x30f/0x380 net/socket.c:744 **sys\_sendmsg+0x903/0xb60 net/socket.c:2602** sys\_sendmsg+0x28d/0x3c0 net/socket.c:2656 \_\_sys\_sendmmsg+0x3c1/0x960 net/socket.c:2742 \_\_do\_sys\_sendmmsg net/socket.c:2771 [inline] \_\_se\_sys\_sendmmsg net/socket.c:2768 [inline] \_\_x64\_sys\_sendmmsg+0xbc/0x120 net/socket.c:2768 x64\_sys\_call+0xb6e/0x3ba0 arch/x86/include/generated/asm/syscalls\_64.h:308 do\_syscall\_x64 arch/x86/entry/common.c:52 [inline] do\_syscall\_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry\_SYSCALL\_64\_after\_hwframe+0x77/0x7f

CPU: 0 UID: 0 PID: 5460 Comm: syz.2.33 Not tainted 6.12.0-rc2-syzkaller-00006-g87d6aab2389e #0  
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024

CVSS v3.1 Base Score	7.1
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H</a>
CWE	CWE-908: Use of Uninitialized Resource

**Vulnerability CVE-2024-50035**

In the Linux kernel, the following vulnerability has been resolved:

ppp: fix ppp\_async\_encode() illegal access

syzbot reported an issue in ppp\_async\_encode() [1]

In this case, pppoe\_sendmsg() is called with a zero size. Then ppp\_async\_encode() is called with an empty skb.

BUG: KMSAN: uninit-value in ppp\_async\_encode drivers/net/ppp/ppp\_async.c:545 [inline]  
 BUG: KMSAN: uninit-value in ppp\_async\_push+0xb4f/0x2660 drivers/net/ppp/ppp\_async.c:675  
 ppp\_async\_encode drivers/net/ppp/ppp\_async.c:545 [inline] ppp\_async\_push+0xb4f/0x2660  
 drivers/net/ppp/ppp\_async.c:675 ppp\_async\_send+0x130/0x1b0 drivers/net/ppp/ppp\_async.c:634  
 ppp\_channel\_bridge\_input drivers/net/ppp/ppp\_generic.c:2280 [inline] ppp\_input+0x1f1/0xe60  
 drivers/net/ppp/ppp\_generic.c:2304 pppoe\_rcv\_core+0x1d3/0x720 drivers/net/ppp/pppoe.c:379  
 sk\_backlog\_rcv+0x13b/0x420 include/net/sock.h:1113 \_\_release\_sock+0x1da/0x330 net/core/  
 sock.c:3072 release\_sock+0x6b/0x250 net/core/sock.c:3626 pppoe\_sendmsg+0x2b8/0xb90 driver-  
 s/net/ppp/pppoe.c:903 sock\_sendmsg\_nosec net/socket.c:729 [inline] \_\_sock\_sendmsg+0x30f/0x380  
 net/socket.c:744 **\_\_sys\_sendmsg+0x903/0xb60 net/socket.c:2602** sys\_sendmsg+0x28d/0x3c0  
 net/socket.c:2656 \_\_sys\_sendmmsg+0x3c1/0x960 net/socket.c:2742 \_\_do\_sys\_sendmmsg net/  
 socket.c:2771 [inline] \_\_se\_sys\_sendmmsg net/socket.c:2768 [inline] \_\_x64\_sys\_sendmmsg+0xbc/0x120  
 net/socket.c:2768 x64\_sys\_call+0xb6e/0x3ba0 arch/x86/include/generated/asm/syscalls\_64.h:308  
 do\_syscall\_x64 arch/x86/entry/common.c:52 [inline] do\_syscall\_64+0xcd/0x1e0 arch/x86/entry/common.c:83  
 entry\_SYSCALL\_64\_after\_hwframe+0x77/0x7f

Uninit was created at: slab\_post\_alloc\_hook mm/slub.c:4092 [inline] slab\_alloc\_node mm/slub.c:4135  
 [inline] kmem\_cache\_alloc\_node\_noprof+0x6bf/0xb80 mm/slub.c:4187 kmalloc\_reserve+0x13d/0x4a0  
 net/core/skbuff.c:587 \_\_alloc\_skb+0x363/0x7b0 net/core/skbuff.c:678 alloc\_skb include/lin-  
 ux/skbuff.h:1322 [inline] sock\_wmalloc+0xfe/0x1a0 net/core/sock.c:2732 pppoe\_sendmsg+0x3a7/0xb90  
 drivers/net/ppp/pppoe.c:867 sock\_sendmsg\_nosec net/socket.c:729 [inline] \_\_sock\_sendmsg+0x30f/0x380  
 net/socket.c:744 **\_\_sys\_sendmsg+0x903/0xb60 net/socket.c:2602** sys\_sendmsg+0x28d/0x3c0  
 net/socket.c:2656 \_\_sys\_sendmmsg+0x3c1/0x960 net/socket.c:2742 \_\_do\_sys\_sendmmsg net/  
 socket.c:2771 [inline] \_\_se\_sys\_sendmmsg net/socket.c:2768 [inline] \_\_x64\_sys\_sendmmsg+0xbc/0x120  
 net/socket.c:2768 x64\_sys\_call+0xb6e/0x3ba0 arch/x86/include/generated/asm/syscalls\_64.h:308  
 do\_syscall\_x64 arch/x86/entry/common.c:52 [inline] do\_syscall\_64+0xcd/0x1e0 arch/x86/entry/common.c:83  
 entry\_SYSCALL\_64\_after\_hwframe+0x77/0x7f

CPU: 1 UID: 0 PID: 5411 Comm: syz.1.14 Not tainted 6.12.0-rc1-syzkaller-00165-g360c1f1f24c6 #0  
 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024

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](#)  
 CWE CWE-908: Use of Uninitialized Resource

**Vulnerability CVE-2024-50039**

In the Linux kernel, the following vulnerability has been resolved:

net/sched: accept TCA\_STAB only for root qdisc

Most qdiscs maintain their backlog using qdisc\_pkt\_len(skb) on the assumption it is invariant between the enqueue() and dequeue() handlers.

Unfortunately syzbot can crash a host rather easily using a TBF + SFQ combination, with an STAB on SFQ [1]

We can't support TCA\_STAB on arbitrary level, this would require to maintain per-qdisc storage.

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-2024-50040**

In the Linux kernel, the following vulnerability has been resolved: igb: Do not bring the device up after non-fatal error.

CVSS v3.1 Base Score 6.2  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H](#)  
CWE CWE-390: Detection of Error Condition Without Action

### **Vulnerability CVE-2024-50044**

In the Linux kernel, the following vulnerability has been resolved:

Bluetooth: RFCOMM: FIX possible deadlock in rfcomm\_sk\_state\_change

rfcomm\_sk\_state\_change attempts to use sock\_lock so it must never be called with it locked but rfcomm\_sock\_ioctl always attempt to lock it.

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](#)  
CWE CWE-667: Improper Locking

### **Vulnerability CVE-2024-50045**

In the Linux kernel, the following vulnerability has been resolved: netfilter: br\_netfilter: fix panic with metadata\_dst skb.

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-2024-50046**

In the Linux kernel, the following vulnerability has been resolved:

NFSv4: Prevent NULL-pointer dereference in nfs42\_complete\_copies()

On the node of an NFS client, some files saved in the mountpoint of the NFS server were copied to another location of the same NFS server. Accidentally, the nfs42\_complete\_copies() got a NULL-pointer dereference crash.

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-2024-50058**

In the Linux kernel, the following vulnerability has been resolved:

serial: protect uart\_port\_dtr\_rts() in uart\_shutdown() too

Commit af224ca2df29 (serial: core: Prevent unsafe uart port access, part 3) added few uport == NULL checks. It added one to uart\_shutdown(), so the commit assumes, uport can be NULL in there. But right after that protection, there is an unprotected "uart\_port\_dtr\_rts(uport, false);" call. That is invoked only if HUPCL is set, so I assume that is the reason why we do not see lots of these reports.

Or it cannot be NULL at this point at all for some reason :P.

Until the above is investigated, stay on the safe side and move this dereference to the if too.

I got this inconsistency from Coverity under CID 1585130. Thanks.

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-2024-50095**

In the Linux kernel, the following vulnerability has been resolved:

RDMA/mad: Improve handling of timed out WRs of mad agent

Current timeout handler of mad agent acquires/releases mad\_agent\_priv lock for every timed out WRs. This causes heavy locking contention when higher no. of WRs are to be handled inside timeout handler.

This leads to softlockup with below trace in some use cases where rdma-cm path is used to establish connection between peer nodes

Simplified timeout handler by creating local list of timed out WRs and invoke send handler post creating the list. The new method acquires/releases lock once to fetch the list and hence helps to reduce locking contetiong when processing higher no. of WRs

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-667: Improper Locking

### **Vulnerability CVE-2024-50121**

nfsd: problematic nfsd\_shrinker\_work using sync mode in nfs4\_state\_shutdown\_net. In the normal case, when we excute `echo 0 > /proc/fs/nfsd/threads`, the function `nfs4_state_destroy_net` in `nfs4_state_shutdown_net` will release all resources related to the hashed `nfs4_client`.

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-416: Use After Free

### **Vulnerability CVE-2024-50127**

In the Linux kernel, the following vulnerability has been resolved:

net: sched: fix use-after-free in taprio\_change()

In 'taprio\_change()', 'admin' pointer may become dangling due to sched switch / removal caused by 'advance\_sched()', and critical section protected by 'q-current\_entry\_lock' is too small to prevent from such a scenario (which causes use-after-free detected by KASAN). Fix this by prefer 'rcu\_replace\_pointer()' ver 'rcu\_assign\_pointer()' to update 'admin' immediately before an attempt to schedule freeing.

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-2024-50131**

In the Linux kernel, the following vulnerability has been resolved:

tracing: Consider the NULL character when validating the event length

strlen() returns a string length excluding the null byte. If the string length equals to the maximum buffer length, the buffer will have no space for the NULL terminating character.

This commit checks this condition and returns failure for it.

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-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

### **Vulnerability CVE-2024-50134**

In the Linux kernel, the following vulnerability has been resolved:

drm/vboxvideo: Replace fake VLA at end of vbva\_mouse\_pointer\_shape with real VLA

Replace the fake VLA at end of the vbva\_mouse\_pointer\_shape shape with a real VLA to fix a “memcpy: detected field-spanning write error”.

Note as mentioned in the added comment it seems the original length calculation for the allocated and send hgsmi buffer is 4 bytes too large. Changing this is not the goal of this patch, so this behavior is kept.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-787: Out-of-bounds Write

### **Vulnerability CVE-2024-50142**

In the Linux kernel, the following vulnerability has been resolved:

xfrm: validate new SA's prefixlen using SA family when sel.family is unset

This expands the validation introduced in commit 07bf7908950a (“xfrm:Validate address prefix lengths in the xfrm selector.”)

syzbot created an SA with usersa.sel.family = AF\_UNSPEC usersa.sel.prefixlen\_s = 128 usersa.family = AF\_INET

Because of the AF\_UNSPEC selector, verify\_newsa\_info doesn't put limits on prefixlen\_s,d. But then copy\_from\_user\_state sets x->sel.family to usersa.family (AF\_INET). Do the same conversion in verify\_newsa\_info before validating prefixlen\_s,d, since that's how prefixlen is going to be used later on.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2024-50148**

In the Linux kernel, the following vulnerability has been resolved:

Bluetooth: bnep: fix wild-memory-access in proto\_unregister

As bnep\_init() ignore bnep\_sock\_init()'s return value, and bnep\_sock\_init() will cleanup all resource. Then when remove bnep module will call bnep\_sock\_cleanup() to cleanup sock's resource. To solve above issue just return bnep\_sock\_init()'s return value in bnep\_exit().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-459: Incomplete Cleanup

### **Vulnerability CVE-2024-50150**

In the Linux kernel, the following vulnerability has been resolved:

usb: typec: altmode should keep reference to parent

The altmode device release refers to its parent device, but without keeping a reference to it.

When registering the altmode, get a reference to the parent and put it in the release function.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

**Vulnerability CVE-2024-50151**

In the Linux kernel, the following vulnerability has been resolved:

smb: client: fix OOBs when building SMB2\_IOCTL request

When using encryption, either enforced by the server or when using 'seal' mount option, the client will squash all compound request buffers down for encryption into a single iov in smb2\_set\_next\_command().

SMB2\_ioctl\_init() allocates a small buffer (448 bytes) to hold the SMB2\_IOCTL request in the first iov, and if the user passes an input buffer that is greater than 328 bytes, smb2\_set\_next\_command() will end up writing off the end of @rqst->iov[0].iov\_base as shown below:

```
mount.cifs //srv/share /mnt -o . . . ,seal ln -s $(perl -e "print('a')for 1..1024") /mnt/link
```

BUG: KASAN: slab-out-of-bounds in smb2\_set\_next\_command.cold+0x1d6/0x24c [cifs] Write of size 4116 at addr ffff8881148fcab8 by task ln/859

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-2024-50153**

In the Linux kernel, the following vulnerability has been resolved:

scsi: target: core: Fix null-ptr-deref in target\_alloc\_device()

There is a null-ptr-deref issue reported by KASAN:

```
BUG: KASAN: null-ptr-deref in target_alloc_device+0xbc4/0xbe0 [target_core_mod] ... kasan_report+0xb9/0xf0
target_alloc_device+0xbc4/0xbe0 [target_core_mod] core_dev_setup_virtual_lun0+0xef/0x1f0 [tar-
get_core_mod] target_core_init_configfs+0x205/0x420 [target_core_mod] do_one_initcall+0xdd/0x4e0
... entry_SYSCALL_64_after_hwframe+0x76/0x7e
```

In target\_alloc\_device(), if allocating memory for dev queues fails, then dev will be freed by dev->transport->free\_device(), but dev->transport is not initialized at that time, which will lead to a null pointer reference problem.

Fixing this bug by freeing dev with hba->backend->ops->free\_device().

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-2024-50188**

net: phy: dp83869: fix memory corruption when enabling fiber. When configuring the fiber port, the DP83869 PHY driver incorrectly calls linkmode\_set\_bit() with a bit mask (1 << 10) rather than a bit number (10). This corrupts some other memory location – in case of arm64 the priv pointer in the same structure.

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-787: Out-of-bounds Write

### **Vulnerability CVE-2024-50205**

In the Linux kernel, the following vulnerability has been resolved:

ALSA: firewire-lib: Avoid division by zero in apply\_constraint\_to\_size()

The step variable is initialized to zero. It is changed in the loop, but if it's not changed it will remain zero. Add a variable check before the division.

The observed behavior was introduced by commit 826b5de90c0b ("ALSA: firewire-lib: fix insufficient PCM rule for period/buffer size"), and it is difficult to show that any of the interval parameters will satisfy the snd\_interval\_test() condition with data from the amdtp\_rate\_table[] table.

Found by Linux Verification Center (linuxtesting.org) with SVACE.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-369: Divide By Zero

### **Vulnerability CVE-2024-50210**

In the Linux kernel, the following vulnerability has been resolved:

posix-clock: posix-clock: Fix unbalanced locking in pc\_clock\_settime()

If get\_clock\_desc() succeeds, it calls fget() for the clockid's fd, and get the clk->rwsem read lock, so the error path should release the lock to make the lock balance and fput the clockid's fd to make the refcount balance and release the fd related resource.

However the below commit left the error path locked behind resulting in unbalanced locking. Check timespec64\_valid\_strict() before get\_clock\_desc() to fix it, because the "ts" is not changed after that.

[pabeni@redhat.com: fixed commit message typo]

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-667: Improper Locking

### **Vulnerability CVE-2024-50251**

In the Linux kernel, the following vulnerability has been resolved: netfilter: nft\_payload: sanitize offset and length before calling skb\_checksum() If access to offset + length is larger than the skbuff length, then skb\_checksum() triggers BUG\_ON(). skb\_checksum() internally subtracts the length parameter while iterating over skbuff, BUG\_ON(len) at the end of it checks that the expected length to be included in the checksum calculation is fully consumed.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-131: Incorrect Calculation of Buffer Size

### **Vulnerability CVE-2024-50262**

In the Linux kernel, the following vulnerability has been resolved: bpf: Fix out-of-bounds write in trie\_get\_next\_key().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-787: Out-of-bounds Write

### **Vulnerability CVE-2024-50299**

In the Linux kernel, the following vulnerability has been resolved: sctp: properly validate chunk size in sctp\_sf\_outb()

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-131: Incorrect Calculation of Buffer Size

### **Vulnerability CVE-2024-50301**

In the Linux kernel, the following vulnerability has been resolved: security/keys: fix slab-out-of-bounds in key\_task\_permission.

CVSS v3.1 Base Score	7.1
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H</a>
CWE	CWE-125: Out-of-bounds Read

### **Vulnerability CVE-2024-50302**

In the Linux kernel, the following vulnerability has been resolved: HID: core: zero-initialize the report buffer Since the report buffer is used by all kinds of drivers in various ways, let's zero-initialize it during allocation to make sure that it can't be ever used to leak kernel memory via specially-crafted report.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-908: Use of Uninitialized Resource

### **Product-Specific Vulnerability Description**

For the following products, the impact of the vulnerability is different.

SIMATIC S7-1500 TM MFP - GNU/Linux subsystem:

The information disclosure is limited to HID driver report data. Successful exploitation requires the installation of malicious code on the device.

CVSS v3.1 Base Score	3.3
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N</a>
CVSS v4.0 Base Score	4.8
CVSS Vector	<a href="#">CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N</a>

### **Vulnerability CVE-2024-53042**

In the Linux kernel, the following vulnerability has been resolved:

ipv4: ip\_tunnel: Fix suspicious RCU usage warning in ip\_tunnel\_init\_flow()

There are code paths from which the function is called without holding the RCU read lock, resulting in a suspicious RCU usage warning [1].

Fix by using l3mdev\_master\_upper\_ifindex\_by\_index() which will acquire the RCU read lock before calling l3mdev\_master\_upper\_ifindex\_by\_index\_rcu().

[1] WARNING: suspicious RCU usage 6.12.0-rc3-custom-gac8f72681cf2 #141 Not tainted

---

net/core/dev.c:876 RCU-list traversed in non-reader section!!

other info that might help us debug this:

rcu\_scheduler\_active = 2, debug\_locks = 1 1 lock held by ip/361: #0: ffffffff86fc7cb0 (rtnl\_mutex)+.-3:3, at: rtnetlink\_rcv\_msg+0x377/0xf60

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-662: Improper Synchronization

### **Vulnerability CVE-2024-53057**

In the Linux kernel, the following vulnerability has been resolved: net/sched: stop qdisc\_tree\_reduce\_backlog on TC\_H\_ROOT.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2024-53059**

In the Linux kernel, the following vulnerability has been resolved:

wifi: iwlmvm: Fix response handling in iwlmvm\_send\_recovery\_cmd()

1. The size of the response packet is not validated.
2. The response buffer is not freed.

Resolve these issues by switching to iwlmvm\_send\_cmd\_status(), which handles both size validation and frees the buffer.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-460: Improper Cleanup on Thrown Exception

### **Vulnerability CVE-2024-53101**

In the Linux kernel, the following vulnerability has been resolved: fs: Fix uninitialized value issue in from\_kuid and from\_kgid ocfs2\_setattr() uses attr->ia\_mode, attr->ia\_uid and attr->ia\_gid in a trace point even though ATTR\_MODE, ATTR\_UID and ATTR\_GID aren't set. Initialize all fields of newattrs to avoid uninitialized variables, by checking if ATTR\_MODE, ATTR\_UID, ATTR\_GID are initialized, otherwise 0.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-456: Missing Initialization of a Variable

### **Vulnerability CVE-2024-53124**

net: fix data-races around sk sk\_forward\_alloc.

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](#)  
CWE CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-56631**

In the Linux kernel, the following vulnerability has been resolved: scsi: sg: Fix slab-use-after-free read in sg\_release() Fix a use-after-free bug in sg\_release(), detected by syzbot with KASAN:

The fix has been tested and validated by syzbot. This patch closes the bug reported at the following syzkaller link and ensures proper sequencing of resource cleanup and mutex operations, eliminating the risk of use-after-free errors in sg\_release().

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-2024-56672**

In the Linux kernel, the following vulnerability has been resolved:

blk-cgroup: Fix UAF in blkcg\_unpin\_online()

blkcg\_unpin\_online() walks up the blkcg hierarchy putting the online pin. To walk up, it uses blkcg\_parent(blkcg) but it was calling that after blkcg\_destroy\_blkgs(blkcg) which could free the blkcg

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-416: Use After Free

### **Vulnerability CVE-2024-57901**

af\_packet: vlan\_get\_protocol\_dgram() vs MSG\_PEEK Blamed allowing a crash.

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-664: Improper Control of a Resource Through its Lifetime

### **Vulnerability CVE-2024-57902**

In the Linux kernel, the following vulnerability has been resolved:

af\_packet: fix vlan\_get\_tci() vs MSG\_PEEK

Blamed commit forgot MSG\_PEEK case, allowing a crash [1] as found by syzbot.

Rework vlan\_get\_tci() to not touch skb at all, so that it can be used from many cpus on the same skb.

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-20: Improper Input Validation

### **Vulnerability CVE-2024-57913**

In the Linux kernel, the following vulnerability has been resolved:

usb: gadget: f\_fs: Remove WARN\_ON in functionfs\_bind

CVSS v3.1 Base Score	4.7
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

### **Vulnerability CVE-2024-57929**

In the Linux kernel, the following vulnerability has been resolved:

dm array: fix releasing a faulty array block twice in dm\_array\_cursor\_end

When dm\_bm\_read\_lock() fails due to locking or checksum errors, it releases the faulty block implicitly while leaving an invalid output pointer behind. The caller of dm\_bm\_read\_lock() should not operate on this invalid dm\_block pointer, or it will lead to undefined result. For example, the dm\_array\_cursor incorrectly caches the invalid pointer on reading a faulty array block, causing a double release in dm\_array\_cursor\_end(), then hitting the BUG\_ON in dm-bufio cache\_put().

CVSS v3.1 Base Score	6.7
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-672: Operation on a Resource after Expiration or Release

### **Vulnerability CVE-2024-57940**

exfat: fix the infinite loop in exfat\_readdir() If the file system is corrupted so that a cluster is linked to itself in the cluster chain, and there is an unused directory entry in the cluster, dentry will not be incremented, causing condition dentry < max\_dentries unable to prevent an infinite loop. This infinite loop causes s\_lock not to be released, and other tasks will hang, such as exfat\_sync\_fs().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

### **Vulnerability CVE-2024-57948**

In the Linux kernel, the following vulnerability has been resolved:

mac802154: check local interfaces before deleting sdata list

syzkaller reported a corrupted list in ieee802154\_if\_remove. [1]

Remove an IEEE 802.15.4 network interface after unregister an IEEE 802.15.4 hardware device from the system.

CVSS v3.1 Base Score	6.7
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

**Vulnerability CVE-2024-57951**

In the Linux kernel, the following vulnerability has been resolved:

hrtimers: Handle CPU state correctly on hotplug

Consider a scenario where a CPU transitions from CPUHP\_ONLINE to halfway through a CPU hotunplug down to CPUHP\_HRTIMERS\_PREPARE, and then back to CPUHP\_ONLINE:

Since hrtimers\_prepare\_cpu() does not run, cpu\_base.hres\_active remains set to 1 throughout. However, during a CPU unplug operation, the tick and the clockevents are shut down at CPUHP\_AP\_TICK\_DYING. On return to the online state, for instance CFS incorrectly assumes that the hrtick is already active, and the chance of the clockevent device to transition to oneshot mode is also lost forever for the CPU, unless it goes back to a lower state than CPUHP\_HRTIMERS\_PREPARE once.

This round-trip reveals another issue; cpu\_base.online is not set to 1 after the transition, which appears as a WARN\_ON\_ONCE in enqueue\_hrtimer().

Aside of that, the bulk of the per CPU state is not reset either, which means there are dangling pointers in the worst case.

Address this by adding a corresponding startup() callback, which resets the stale per CPU state and sets the online flag.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

**Vulnerability CVE-2024-57977**

memcg: A soft lockup vulnerability in the product with about 56,000 tasks were in the OOM cgroup, it was traversing them when the soft lockup was triggered.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-667: Improper Locking

**Vulnerability CVE-2024-57979**

pps: Fix a use-after-free

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

**Vulnerability CVE-2024-57981**

usb: xhci: NULL pointer dereference on certain command aborts. If a command is queued to the final usable TRB of a ring segment, the enqueue pointer is advanced to the subsequent link TRB and no further. If the command is later aborted, when the abort completion is handled the dequeue pointer is advanced to the first TRB of the next segment. If no further commands are queued, xhci\_handle\_stopped\_cmd\_ring() sees the ring pointers unequal and assumes that there is a pending command, so it calls xhci\_mod\_cmd\_timer() which crashes if cur\_cmd was NULL.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2024-57986**

HID: core: Fix assumption that Resolution Multipliers must be in Logical Collections

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-20: Improper Input Validation

**Vulnerability CVE-2024-58005**

tpm: Change to kcalloc() in eventlog/acpi.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](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-58009**

Bluetooth: L2CAP: handle NULL sock pointer in l2cap\_sock\_alloc

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-20: Improper Input Validation

**Vulnerability CVE-2024-58014**

wifi: brcmsmac: add gain range check to wlc\_phy\_iqcal\_gainparams\_nphy()

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:N/A:H](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-58016**

safesetid: check size of policy writes

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-20: Improper Input Validation

**Vulnerability CVE-2024-58017**

printk: Fix signed integer overflow when defining LOG\_BUF\_LEN\_MAX

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-190: Integer Overflow or Wraparound

**Vulnerability CVE-2024-58020**

HID: multitouch: Add NULL check in mt\_input\_configured

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-2024-58051**

ipmi: ipmb: Add check devm\_kasprintf() returned value

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-20: Improper Input Validation

**Vulnerability CVE-2024-58058**

ubifs: skip dumping tnc tree when zroot is null

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-2024-58063**

wifi: rtlwifi: fix memory leaks and invalid access at probe error path

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-401: Missing Release of Memory after Effective Lifetime

**Vulnerability CVE-2024-58071**

team: prevent adding a device which is already a team device lower

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-667: Improper Locking

**Vulnerability CVE-2024-58072**

wifi: rtlwifi: remove unused check\_buddy\_priv

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](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2024-58085**

tomoyo: don't emit warning in tomoyo\_write\_control()

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-20: Improper Input Validation

**Vulnerability CVE-2025-9230**

An application trying to decrypt CMS messages encrypted using password based encryption can trigger an out-of-bounds read and write. Impact summary: This out-of-bounds read may trigger a crash which leads to Denial of Service for an application. The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service or Execution of attacker-supplied code. Although the consequences of a successful exploit of this vulnerability could be severe, the probability that the attacker would be able to perform it is low. Besides, password based (PWRI) encryption support in CMS messages is very rarely used. For that reason the issue was assessed as Moderate severity according to our Security Policy. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary.

CVSS v3.1 Base Score 5.6  
CVSS Vector [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L](#)  
CWE CWE-787: Out-of-bounds Write

### **Vulnerability CVE-2025-21638**

In the Linux kernel, the following vulnerability has been resolved:

sctp: sysctl: auth\_enable: avoid using current->nsproxy

As mentioned in a previous commit of this series, using the 'net' structure via 'current' is not recommended for different reasons:

- Inconsistency: getting info from the reader's/writer's netns vs only from the opener's netns.
- current->nsproxy can be NULL in some cases, resulting in an 'Oops' (null-ptr-deref), e.g. when the current task is exiting, as spotted by syzbot [1] using acct(2).

The 'net' structure can be obtained from the table->data using container\_of().

Note that table->data could also be used directly, but that would increase the size of this fix, while 'sctpctl\_sock' still needs to be retrieved from 'net' structure.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

### **Vulnerability CVE-2025-21639**

In the Linux kernel, the following vulnerability has been resolved:

sctp: sysctl: rto\_min/max: avoid using current->nsproxy

As mentioned in a previous commit of this series, using the 'net' structure via 'current' is not recommended for different reasons:

- Inconsistency: getting info from the reader's/writer's netns vs only from the opener's netns.
- current->nsproxy can be NULL in some cases, resulting in an 'Oops' (null-ptr-deref), e.g. when the current task is exiting, as spotted by syzbot [1] using acct(2).

The 'net' structure can be obtained from the table->data using container\_of().

Note that table->data could also be used directly, as this is the only member needed from the 'net' structure, but that would increase the size of this fix, to use '\*data' everywhere 'net->sctp.rto\_min/max' is used.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

### **Vulnerability CVE-2025-21640**

In the Linux kernel, the following vulnerability has been resolved:

sctp: sysctl: cookie\_hmac\_alg: avoid using current->nsproxy

As mentioned in a previous commit of this series, using the 'net' structure via 'current' is not recommended for different reasons:

- Inconsistency: getting info from the reader's/writer's netns vs only from the opener's netns.
- current->nsproxy can be NULL in some cases, resulting in an 'Oops' (null-ptr-deref), e.g. when the current task is exiting, as spotted by syzbot [1] using acct(2).

The 'net' structure can be obtained from the table->data using container\_of().

Note that table->data could also be used directly, as this is the only member needed from the 'net' structure, but that would increase the size of this fix, to use '\*data' everywhere 'net->sctp.sctp\_hmac\_alg' is used.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

### **Vulnerability CVE-2025-21647**

In the Linux kernel, the following vulnerability has been resolved: sched: sch\_cake: add bounds checks to host bulk flow fairness counts

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](#)  
CWE CWE-125: Out-of-bounds Read

### **Vulnerability CVE-2025-21648**

In the Linux kernel, the following vulnerability has been resolved:

netfilter: conntrack: clamp maximum hashtable size to INT\_MAX

Use INT\_MAX as maximum size for the conntrack hashtable. Otherwise, it is possible to hit WARN\_ON\_ONCE in \_\_kvmalloc\_node\_noprof() when resizing hashtable because \_\_GFP\_NOWARN is unset. See:

0708a0afe291 ("mm: Consider \_\_GFP\_NOWARN flag for oversized kvmalloc() calls")

Note: hashtable resize is only possible from init\_netns.

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-789: Memory Allocation with Excessive Size Value

### **Vulnerability CVE-2025-21653**

net\_sched: cls\_flow: validate TCA\_FLOW\_RSHIFT attribute

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](#)  
CWE CWE-20: Improper Input Validation

### **Vulnerability CVE-2025-21664**

dm thin: make get\_first\_thin use rcu-safe list first function

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-20: Improper Input Validation

### **Vulnerability CVE-2025-21666**

vsock: prevent null-ptr-deref in vsock\_has\_data|has\_space

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-2025-21669**

vsock/virtio: discard packets if the transport changes

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-2025-21678**

gtp: Destroy device along with udp socket's netns dismantle

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-20: Improper Input Validation

### **Vulnerability CVE-2025-21683**

bpf: Fix bpf\_sk\_select\_reuseport() memory leak

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-401: Missing Release of Memory after Effective Lifetime

### **Vulnerability CVE-2025-21692**

net: sched: fix ets qdisc OOB Indexing

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-129: Improper Validation of Array Index

### **Vulnerability CVE-2025-21694**

fs/proc: softlockup in \_\_read\_vmcore

CVSS v3.1 Base Score 4.1  
CVSS Vector [CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H](#)  
CWE CWE-667: Improper Locking

### **Vulnerability CVE-2025-21704**

usb: cdc-acm: Check control transfer buffer size before access

CVSS v3.1 Base Score 4.4  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H](#)  
CVSS v4.0 Base Score 4.1  
CVSS Vector [CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:P/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N](#)  
CWE CWE-20: Improper Input Validation

### **Vulnerability CVE-2025-21711**

net/rose: prevent integer overflows in rose\_setsockopt()

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-190: Integer Overflow or Wraparound

### **Vulnerability CVE-2025-21719**

ipmr: do not call mr\_mfc\_uses\_dev() for unres entries

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-20: Improper Input Validation

### **Vulnerability CVE-2025-21726**

padata: avoid UAF for reorder\_work

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2025-21727**

padata: fix UAF in padata\_reorder

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2025-21728**

bpf: Send signals asynchronously if !preemptible BPF programs can execute in all kinds of contexts and when a program running in a non-preemptible context uses the bpf\_send\_signal() kfunc, it will cause issues because this kfunc can sleep.

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2025-21735**

NFC: nci: Add bounds checking in nci\_hci\_create\_pipe()

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-787: Out-of-bounds Write

### **Vulnerability CVE-2025-21744**

wifi: brcmfmac: fix NULL pointer dereference in brcmf\_txfinalize()

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-476: NULL Pointer Dereference

### **Vulnerability CVE-2025-21745**

In the Linux kernel, the following vulnerability has been resolved:

blk-cgroup: Fix class @block\_class's subsystem refcount leakage

blkcg\_fill\_root\_iostats() iterates over @block\_class's devices by class\_dev\_iter\_(init|next)(), but does not end iterating with class\_dev\_iter\_exit(), so causes the class's subsystem refcount leakage.

Fix by ending the iterating with class\_dev\_iter\_exit().

CVSS v3.1 Base Score	5.5
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2025-21753**

btrfs: fix use-after-free when attempting to join an aborted transaction

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-416: Use After Free

### **Vulnerability CVE-2025-21756**

vsock: Keep the binding until socket destruction Preserve sockets bindings; this includes both resulting from an explicit bind() and those implicitly bound through autobind during connect().

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-20: Improper Input Validation

### **Vulnerability CVE-2025-21760**

ndisc: extend RCU protection in ndisc\_send\_skb()

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-2025-21761**

openvswitch: use RCU protection in ovs\_vport\_cmd\_fill\_info()

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-2025-21762**

In the Linux kernel, the following vulnerability has been resolved: arp: use RCU protection in arp\_xmit() arp\_xmit() can be called without RTNL or RCU protection. Use RCU protection to avoid potential UAF.

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-20: Improper Input Validation

### **Vulnerability CVE-2025-21763**

neighbour: use RCU protection in \_\_neigh\_notify()

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-2025-21764**

ndisc: use RCU protection in ndisc\_alloc\_skb()

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-2025-21765**

ipv6: use RCU protection in ip6\_default\_advmss() ip6\_default\_advmss() needs rcu protection to make sure the net structure it reads does not disappear.

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-20: Improper Input Validation

**Vulnerability CVE-2025-21772**

partitions: mac: fix handling of bogus partition table

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](#)  
CWE CWE-20: Improper Input Validation

**Vulnerability CVE-2025-21776**

USB: hub: Ignore non-compliant devices with too many configs or interfaces. A test program can cause `usb_hub_to_struct_hub()` to dereference a NULL or inappropriate pointer.

CVSS v3.1 Base Score 4.4  
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H](#)  
CWE CWE-476: NULL Pointer Dereference

**Vulnerability CVE-2025-21787**

team: better `TEAM_OPTION_TYPE_STRING` validation

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-908: Use of Uninitialized Resource

**Vulnerability CVE-2025-21795**

NFSD: hang in `nfsd4_shutdown_callback`. If `nfs4_client` is in courtesy state then there is no point to send the callback. This causes `nfsd4_shutdown_callback` to hang since `cl_cb_inflight` is not 0. This hang lasts about 15 minutes until TCP notifies NFSD that the connection was dropped.

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-20: Improper Input Validation

**Vulnerability CVE-2025-21796**

nfsd: clear `acl_access/acl_default` after releasing them. If getting `acl_default` fails, `acl_access` and `acl_default` will be released simultaneously.

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-20: Improper Input Validation

**Vulnerability CVE-2025-21806**

net: let `net.core.dev_weight` always be non-zero. The following problem was encountered during stability test: (NULL `net_device`).

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-20: Improper Input Validation

**Vulnerability CVE-2025-21814**

ptp: Ensure `info->enable` callback is always set

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-2025-21826**

netfilter: nf\_tables: reject mismatching sum of field\_len with set key length. The field length description provides the length of each separated key field in the concatenation, each field gets rounded up to 32-bits to calculate the pipapo rule width from pipapo\_init(). The set key length provides the total size of the key aligned to 32-bits. Register-based arithmetics still allows for combining mismatching set key length and field length description, eg. set key length 10 and field description [ 5, 4 ] leading to pipapo width of 12.

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-20: Improper Input Validation

**Vulnerability CVE-2025-21835**

usb: gadget: f\_midi: fix MIDI Streaming descriptor lengths

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-20: Improper Input Validation

**Vulnerability CVE-2025-21844**

smb: client: Add check for next\_buffer in receive\_encrypted\_standard()

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-2025-21846**

acct: perform last write from workqueue

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-2025-21858**

geneve: Fix use-after-free in geneve\_find\_dev()

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-2025-21859**

USB: gadget: f\_midi: f\_midi\_complete to call queue\_work

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-667: Improper Locking

**Vulnerability CVE-2025-21862**

drop\_monitor: incorrect initialization order. If drop\_monitor is built as a kernel module, syzkaller may have time to send a netlink NET\_DM\_CMD\_START message during the module loading. This will call the net\_dm\_monitor\_start() function that uses a spinlock that has not yet been initialized.

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-908: Use of Uninitialized Resource

### **Vulnerability CVE-2025-21865**

gtp: Suppress list corruption splat in gtp\_net\_exit\_batch\_rtnl(). Commit eb28fd76c0a0 ("gtp: Destroy device along with udp socket's netns dismantle.") added the for\_each\_netdev() loop in gtp\_net\_exit\_batch\_rtnl() to destroy devices in each netns as done in geneve and ip tunnels. However, this could trigger ->dellink() twice for the same device during ->exit\_batch\_rtnl().

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-787: Out-of-bounds Write

### **ADDITIONAL INFORMATION**

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 (2024-04-09):	Publication Date
V1.1 (2024-05-14):	Added CVE-2024-2511
V1.2 (2024-07-09):	Added CVE-2024-5535
V1.3 (2024-11-12):	Added CVE-2024-9143
V1.4 (2025-03-11):	Added CVE-2024-36484, CVE-2024-36902, CVE-2024-36904, CVE-2024-36905, CVE-2024-36916, CVE-2024-36929, CVE-2024-36939, CVE-2024-36940, CVE-2024-36959, CVE-2024-44987, CVE-2024-44989, CVE-2024-44990, CVE-2024-45016, CVE-2024-45018, CVE-2024-46679, CVE-2024-46743, CVE-2024-46744, CVE-2024-46745, CVE-2024-46750, CVE-2024-46759, CVE-2024-46783, CVE-2024-47660, CVE-2024-50299, CVE-2024-50301, CVE-2024-53101
V1.5 (2025-04-08):	Added CVE-2024-50302 (incl. product-specific impact description) and multiple other CVEs
V1.6 (2025-06-10):	Added 63 CVEs
V1.7 (2025-07-08):	Added 71 CVEs
V1.8 (2025-08-12):	Added 147 CVEs
V1.9 (2025-09-09):	Added 51 CVEs
V2.0 (2025-10-14):	Added CVE-2025-9230, CVE-2023-50781, CVE-2023-6129, CVE-2023-6237, CVE-2024-0727

### **TERMS OF USE**

The use of Siemens Security Advisories is subject to the terms and conditions listed on: <https://www.siemens.com/productcert/terms-of-use>.