SSA-419740: Multiple Third-Party Component Vulnerabilities in RUGGEDCOM and SCALANCE Products before V7.2

Publication Date: 2023-03-14
Last Update: 2023-03-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Multiple third-party component vulnerabilities were reported for the Busybox applet, the Linux Kernel, OpenSSL, OpenVPN and various other components used by the RUGGEDCOM and SCALANCE products. The vulnerabilities range from improper neutralization of special elements to improper handling of commands under certain circumstances, that could lead to code injection and denial of service.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M812-1 ADSL-Router (Annex A) (6GK5812-1AA00-2AA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M812-1 ADSL-Router (Annex B) (6GK5812-1BA00-2AA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M816-1 ADSL-Router (Annex A) (6GK5816-1AA00-2AA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M816-1 ADSL-Router (Annex B) (6GK5816-1BA00-2AA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/

SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M876-3 (EVDO) (6GK5876-3AA02-2BA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M876-4 (6GK5876-4AA10-2BA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE MUM853-1 (EU) (6GK5853-2EA00-2DA1): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE S615 (6GK5615-0AA00-2AA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/
SCALANCE S615 EEC (6GK5615-0AA01-2AA2): All versions < V7.2	Update to V7.2 or later version https://support.industry.siemens.com/cs/document/109817007/

WORKAROUNDS AND MITIGATIONS

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

GENERAL SECURITY RECOMMENDATIONS

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

PRODUCT DESCRIPTION

SCALANCE M-800, MUM-800 and S615 as well as the RUGGEDCOM RM1224 are industrial routers.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2018-25032

zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2019-1125

An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2021-4034

A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

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

Vulnerability CVE-2021-4149

A vulnerability was found in btrfs_alloc_tree_b in fs/btrfs/extent-tree.c in the Linux kernel due to an improper lock operation in btrfs. In this flaw, a user with a local privilege may cause a denial of service (DOS) due to a deadlock problem.

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

Vulnerability CVE-2021-26401

LFENCE/JMP (mitigation V2-2) may not sufficiently mitigate CVE-2017-5715 on some AMD CPUs.

CVSS v3.1 Base Score	5.6
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-42373

A NULL pointer dereference in Busybox's man applet leads to denial of service when a section name is supplied but no page argument is given.

CVSS v3.1 Base Score	5.1
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2021-42374

An out-of-bounds heap read in Busybox's unlzma applet leads to information leak and denial of service when crafted LZMA-compressed input is decompressed. This can be triggered by any applet/format that internally supports LZMA compression.

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

Vulnerability CVE-2021-42375

An incorrect handling of a special element in Busybox's ash applet leads to denial of service when processing a crafted shell command, due to the shell mistaking specific characters for reserved characters. This may be used for DoS under rare conditions of filtered command input.

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/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-42376

A NULL pointer dereference in Busybox's hush applet leads to denial of service when processing a crafted shell command, due to missing validation after a \x03 delimiter character. This may be used for DoS under very rare conditions of filtered command input.

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/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2021-42377

An attacker-controlled pointer free in Busybox's hush applet leads to denial of service and possible code execution when processing a crafted shell command, due to the shell mishandling the &&& string. This may be used for remote code execution under rare conditions of filtered command input.

CVSS v3.1 Base Score	6.4
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-763: Release of Invalid Pointer or Reference

Vulnerability CVE-2021-42378

A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the getvar_i function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42379

A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the next_input_file function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42380

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the clrvar function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42381

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the hash_init function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42382

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the getvar_s function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42383

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the evaluate function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42384

A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the handle_special function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42385

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the evaluate function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42386

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the nvalloc function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-0001

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

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

Vulnerability CVE-2022-0002

Non-transparent sharing of branch predictor within a context in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.

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

Vulnerability CVE-2022-0494

A kernel information leak flaw was identified in the scsi_ioctl function in drivers/scsi/scsi_ioctl.c in the Linux kernel. This flaw allows a local attacker with a special user privilege (CAP_SYS_ADMIN or CAP_SYS_RAWIO) to create issues with confidentiality.

CVSS v3.1 Base Score	4.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2022-0547

OpenVPN 2.1 until v2.4.12 and v2.5.6 may enable authentication bypass in external authentication plug-ins when more than one of them makes use of deferred authentication replies, which allows an external user to be granted access with only partially correct credentials.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2022-1011

A use-after-free flaw was found in the Linux kernel's FUSE filesystem in the way a user triggers write(). This flaw allows a local user to gain unauthorized access to data from the FUSE filesystem, resulting in privilege escalation.

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

Vulnerability CVE-2022-1016

A flaw was found in the Linux kernel in net/netfilter/nf_tables_core.c:nft_do_chain, which can cause a use-after-free. This issue needs to handle 'return' with proper preconditions, as it can lead to a kernel information leak problem caused by a local, unprivileged attacker.

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

Vulnerability CVE-2022-1198

A use-after-free vulnerabilitity was discovered in drivers/net/hamradio/6pack.c of linux that allows an attacker to crash linux kernel by simulating ax25 device using 6pack driver from user 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/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-1199

A flaw was found in the Linux kernel. This flaw allows an attacker to crash the Linux kernel by simulating amateur radio from the user space, resulting in a null-ptr-deref vulnerability and a use-after-free vulnerability.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-1292

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

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

Vulnerability CVE-2022-1304

An out-of-bounds read/write vulnerability was found in e2fsprogs 1.46.5. This issue leads to a segmentation fault and possibly arbitrary code execution via a specially crafted filesystem.

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

Vulnerability CVE-2022-1343

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

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

Vulnerability CVE-2022-1353

A vulnerability was found in the pfkey_register function in net/key/af_key.c in the Linux kernel. This flaw allows a local, unprivileged user to gain access to kernel memory, leading to a system crash or a leak of internal kernel information.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2022-1473

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

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

Vulnerability CVE-2022-1516

A NULL pointer dereference flaw was found in the Linux kernel's X.25 set of standardized network protocols functionality in the way a user terminates their session using a simulated Ethernet card and continued usage of this connection. This flaw allows a local user to crash the system.

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

Vulnerability CVE-2022-1652

Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a concurrency use-after-free flaw in the bad_flp_intr function. By executing a specially-crafted program, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

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

Vulnerability CVE-2022-1729

A race condition was found the Linux kernel in perf_event_open() which can be exploited by an unprivileged user to gain root privileges. The bug allows to build several exploit primitives such as kernel address information leak, arbitrary execution, etc.

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

Vulnerability CVE-2022-1734

A flaw in Linux Kernel found in nfcmrvl_nci_unregister_dev() in drivers/nfc/nfcmrvl/main.c can lead to use after free both read or write when non synchronized between cleanup routine and firmware download routine.

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

Vulnerability CVE-2022-1974

A use-after-free flaw was found in the Linux kernel's NFC core functionality due to a race condition between kobject creation and delete. This vulnerability allows a local attacker with CAP_NET_ADMIN privilege to leak kernel information.

CVSS v3.1 Base Score	4.1
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-1975

There is a sleep-in-atomic bug in /net/nfc/netlink.c that allows an attacker to crash the Linux kernel by simulating a nfc device from user-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/E:P/RL:O/RC:C
CWE	CWE-248: Uncaught Exception

Vulnerability CVE-2022-2380

The Linux kernel was found vulnerable out of bounds memory access in the drivers/video/fbdev/sm712fb.c:smtcfb_read() function. The vulnerability could result in local attackers being able to crash the kernel.

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

Vulnerability CVE-2022-2588

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

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

Vulnerability CVE-2022-2639

An integer coercion error was found in the openvswitch kernel module. Given a sufficiently large number of actions, while copying and reserving memory for a new action of a new flow, the reserve_sfa_size() function does not return -EMSGSIZE as expected, potentially leading to an out-of-bounds write access. This flaw allows a local user to crash or potentially escalate their privileges on the system.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-191: Integer Underflow (Wrap or Wraparound)

Vulnerability CVE-2022-20158

In bdi_put and bdi_unregister of backing-dev.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-182815710References: Upstream kernel

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

Vulnerability CVE-2022-23036

Linux PV device frontends vulnerable to attacks by backends [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend.

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

Vulnerability CVE-2022-23037

Linux PV device frontends vulnerable to attacks by backends [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend.

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

Vulnerability CVE-2022-23038

Linux PV device frontends vulnerable to attacks by backends [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend.

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

Vulnerability CVE-2022-23039

Linux PV device frontends vulnerable to attacks by backends [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend.

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

Vulnerability CVE-2022-23040

Linux PV device frontends vulnerable to attacks by backends [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend.

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

Vulnerability CVE-2022-23041

Linux PV device frontends vulnerable to attacks by backends [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend.

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

Vulnerability CVE-2022-23042

Linux PV device frontends vulnerable to attacks by backends [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Several Linux PV device frontends are using the grant table interfaces for removing access rights of the backends in ways being subject to race conditions, resulting in potential data leaks, data corruption by malicious backends, and denial of service triggered by malicious backends: blkfront, netfront, scsifront and the gntalloc driver are testing whether a grant reference is still in use. If this is not the case, they assume that a following removal of the granted access will always succeed, which is not true in case the backend has mapped the granted page between those two operations. As a result the backend can keep access to the memory page of the guest no matter how the page will be used after the frontend I/O has finished. The xenbus driver has a similar problem, as it doesn't check the success of removing the granted access of a shared ring buffer. blkfront: CVE-2022-23036 netfront: CVE-2022-23037 scsifront: CVE-2022-23038 gntalloc: CVE-2022-23039 xenbus: CVE-2022-23040 blkfront, netfront, scsifront, usbfront, dmabuf, xenbus, 9p, kbdfront, and pvcalls are using a functionality to delay freeing a grant reference until it is no longer in use, but the freeing of the related data page is not synchronized with dropping the granted access. As a result the backend can keep access to the memory page even after it has been freed and then re-used for a different purpose. CVE-2022-23041 netfront will fail a BUG_ON() assertion if it fails to revoke access in the rx path. This will result in a Denial of Service (DoS) situation of the guest which can be triggered by the backend.

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

Vulnerability CVE-2022-23308

valid.c in libxml2 before 2.9.13 has a use-after-free of ID and IDREF attributes.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-26490

st21nfca_connectivity_event_received in drivers/nfc/st21nfca/se.c in the Linux kernel through 5.16.12 has EVT_TRANSACTION buffer overflows because of untrusted length parameters.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-28356

In the Linux kernel before 5.17.1, a refcount leak bug was found in net/llc/af_llc.c.

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

Vulnerability CVE-2022-28390

ems_usb_start_xmit in drivers/net/can/usb/ems_usb.c in the Linux kernel through 5.17.1 has a double free.

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

Vulnerability CVE-2022-30065

A use-after-free in Busybox 1.35-x's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the copyvar function.

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

Vulnerability CVE-2022-30594

The Linux kernel before 5.17.2 mishandles seccomp permissions. The PTRACE_SEIZE code path allows attackers to bypass intended restrictions on setting the PT_SUSPEND_SECCOMP flag.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-863: Incorrect Authorization

Vulnerability CVE-2022-32205

A malicious server can serve excessive amounts of "Set-Cookie:" headers in a HTTP response to curl and curl < 7.84.0 stores all of them. A sufficiently large amount of (big) cookies make subsequent HTTP requests to this, or other servers to which the cookies match, create requests that become larger than the threshold that curl uses internally to avoid sending crazy large requests (1048576 bytes) and instead returns an error.This denial state might remain for as long as the same cookies are kept, match and haven't expired. Due to cookie matching rules, a server on "foo.example.com" can set cookies that also would match for "bar.example.com", making it it possible for a "sister server" to effectively cause a denial of service for a sibling site on the same second level domain using this method.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2022-32206

curl < 7.84.0 supports "chained" HTTP compression algorithms, meaning that a serverresponse can be compressed multiple times and potentially with different algorithms. The number of acceptable "links" in this "decompression chain" was unbounded, allowing a malicious server to insert a virtually unlimited number of compression steps.The use of such a decompression chain could result in a "malloc bomb", makingcurl end up spending enormous amounts of allocated heap memory, or trying toand returning out of memory errors.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2022-32207

When curl < 7.84.0 saves cookies, alt-svc and hsts data to local files, it makes the operation atomic by finalizing the operation with a rename from a temporary name to the final target file name.In that rename operation, it might accidentally *widen* the permissions for the target file, leaving the updated file accessible to more users than intended.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-276: Incorrect Default Permissions

Vulnerability CVE-2022-32208

When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw makes it possible for a Man-In-The-Middle attack to go unnoticed and even allows it to inject data to the client.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-32296

The Linux kernel before 5.17.9 allows TCP servers to identify clients by observing what source ports are used. This occurs because of use of Algorithm 4 ("Double-Hash Port Selection Algorithm") of RFC 6056.

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

Vulnerability CVE-2022-32981

An issue was discovered in the Linux kernel through 5.18.3 on powerpc 32-bit platforms. There is a buffer overflow in ptrace PEEKUSER and POKEUSER (aka PEEKUSR and POKEUSR) when accessing floating point registers.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input (’Classic Buffer Overflow’)

Vulnerability CVE-2022-33981

drivers/block/floppy.c in the Linux kernel before 5.17.6 is vulnerable to a denial of service, because of a concurrency use-after-free flaw after deallocating raw_cmd in the raw_cmd_ioctl function.

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-35252

When curl is used to retrieve and parse cookies from a HTTP(S) server, itaccepts cookies using control codes that when later are sent back to a HTTPserver might make the server return 400 responses. Effectively allowing a"sister site” to deny service to all siblings.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
CWE	CWE-1286: Improper Validation of Syntactic Correctness of Input

Vulnerability CVE-2022-36879

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

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

Vulnerability CVE-2022-36946

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

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

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 (2023-03-14): Publication Date

TERMS OF USE