

## **SSA-831302: Vulnerabilities in the BIOS of the SIMATIC S7-1500 TM MFP before V1.3.0**

Publication Date: 2023-06-13  
Last Update: 2024-04-09  
Current Version: V1.4  
CVSS v3.1 Base Score: 9.8

### **SUMMARY**

Multiple vulnerabilities have been identified in the BIOS of the SIMATIC S7-1500 TM MFP before V1.3.0. Siemens has released a new version for SIMATIC S7-1500 TM MFP - BIOS and recommends to update to the latest version.

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
SIMATIC S7-1500 TM MFP - BIOS: All versions < V1.3.0 affected by <a href="#">all CVEs</a>	Update to V1.3.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109945851/">https://support.industry.siemens.com/cs/ww/en/view/109945851/</a> See further 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

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

### **GENERAL SECURITY RECOMMENDATIONS**

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

## **PRODUCT DESCRIPTION**

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

## **VULNERABILITY DESCRIPTION**

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

### **Vulnerability CVE-2016-10228**

The iconv program in the GNU C Library (aka glibc or libc6) 2.31 and earlier, when invoked with multiple suffixes in the destination encoding (TRANSLATE or IGNORE) along with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.

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

### **Vulnerability CVE-2019-25013**

The iconv feature in the GNU C Library (aka glibc or libc6) through 2.32, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.

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/E:P/RL:O/RC:C</a>
CWE	CWE-125: Out-of-bounds Read

### **Vulnerability CVE-2020-1752**

A use-after-free vulnerability introduced in glibc upstream version 2.14 was found in the way the tilde expansion was carried out. Directory paths containing an initial tilde followed by a valid username were affected by this issue. A local attacker could exploit this flaw by creating a specially crafted path that, when processed by the glob function, would potentially lead to arbitrary code execution. This was fixed in version 2.32.

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

### **Vulnerability CVE-2020-10029**

The GNU C Library (aka glibc or libc6) before 2.32 could overflow an on-stack buffer during range reduction if an input to an 80-bit long double function contains a non-canonical bit pattern, as seen when passing a 0x5d414141414141410000 value to sinl on x86 targets. This is related to sysdeps/ieee754/dbl-96/e\_rem\_pio2l.c.

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/E:P/RL:O/RC:C</a>
CWE	CWE-787: Out-of-bounds Write

**Vulnerability CVE-2020-27618**

The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid multi-byte input sequences in IBM1364, IBM1371, IBM1388, IBM1390, and IBM1399 encodings, fails to advance the input state, which could lead to an infinite loop in applications, resulting in a denial of service, a different vulnerability from CVE-2016-10228.

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

**Vulnerability CVE-2020-29562**

The iconv function in the GNU C Library (aka glibc or libc6) 2.30 to 2.32, when converting UCS4 text containing an irreversible character, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.

CVSS v3.1 Base Score 4.8  
CVSS Vector [CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C](#)  
CWE CWE-617: Reachable Assertion

**Vulnerability CVE-2021-3326**

The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid input sequences in the ISO-2022-JP-3 encoding, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.

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-617: Reachable Assertion

**Vulnerability CVE-2021-3998**

A flaw was found in glibc. The realpath() function can mistakenly return an unexpected value, potentially leading to information leakage and disclosure of 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/E:P/RL:O/RC:C](#)  
CWE CWE-125: Out-of-bounds Read

**Vulnerability CVE-2021-3999**

A flaw was found in glibc. An off-by-one buffer overflow and underflow in getcwd() may lead to memory corruption when the size of the buffer is exactly 1. A local attacker who can control the input buffer and size passed to getcwd() in a setuid program could use this flaw to potentially execute arbitrary code and 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-193: Off-by-one Error

**Vulnerability CVE-2021-20269**

A flaw was found in the permissions of a log file created by kexec-tools. This flaw allows a local unprivileged user to read this file and leak kernel internal information from a previous panic. The highest threat from this vulnerability is to confidentiality. This flaw affects kexec-tools shipped by Fedora versions prior to 2.0.21-8 and RHEL versions prior to 2.0.20-47.

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-276: Incorrect Default Permissions

**Vulnerability CVE-2021-27645**

The nameserver caching daemon (nscd) in the GNU C Library (aka glibc or libc6) 2.29 through 2.33, when processing a request for netgroup lookup, may crash due to a double-free, potentially resulting in degraded service or Denial of Service on the local system. This is related to netgroupcache.c.

CVSS v3.1 Base Score 2.5  
CVSS Vector [CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C](#)  
CWE CWE-415: Double Free

**Vulnerability CVE-2021-28831**

decompress\_gunzip.c in BusyBox through 1.32.1 mishandles the error bit on the huft\_build result pointer, with a resultant invalid free or segmentation fault, via malformed gzip data.

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-755: Improper Handling of Exceptional Conditions

**Vulnerability CVE-2021-33574**

The mq\_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application crash) or possibly unspecified other impact.

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:N/A:H/E:P/RL:O/RC:C](#)  
CWE CWE-416: Use After Free

**Vulnerability CVE-2021-35942**

The wordexp function in the GNU C Library (aka glibc) through 2.33 may crash or read arbitrary memory in parse\_param (in posix/wordexp.c) when called with an untrusted, crafted pattern, potentially resulting in a denial of service or disclosure of information. This occurs because atoi was used but strtoul should have been used to ensure correct calculations.

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/E:P/RL:O/RC:C](#)  
CWE CWE-190: Integer Overflow or Wraparound

**Vulnerability CVE-2021-38604**

In librt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/sysv/linux/mq\_notify.c mishandles certain NOTIFY\_REMOVED data, leading to a NULL pointer dereference. NOTE: this vulnerability was introduced as a side effect of the CVE-2021-33574 fix.

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-476: NULL Pointer Dereference

**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-2021-44879**

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

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

**Vulnerability CVE-2022-1015**

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

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

**Vulnerability CVE-2022-1882**

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

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

**Vulnerability CVE-2022-2585**

A use-after-free flaw was found in the Linux kernel's POSIX CPU timers functionality in the way a user creates and then deletes the timer in the non-leader thread of the program. This flaw allows a local user to crash or potentially escalate their privileges on the system.

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

**Vulnerability CVE-2022-2588**

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-2022-2905**

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

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

**Vulnerability CVE-2022-3028**

A race condition was found in the Linux kernel's IP framework for transforming packets (XFRM subsystem) when multiple calls to `xfrm_probe_algs` occurred simultaneously. This flaw could allow a local attacker to potentially trigger an out-of-bounds write or leak kernel heap memory by performing an out-of-bounds read and copying it into a socket.

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

**Vulnerability CVE-2022-3435**

A vulnerability classified as problematic has been found in Linux Kernel. This affects the function `fib_nh_match` of the file `net/ipv4/fib_semantics.c` of the component IPv4 Handler. The manipulation leads to out-of-bounds read. It is possible to initiate the attack remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-210357 was assigned to this vulnerability.

CVSS v3.1 Base Score 4.3  
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C](#)  
CWE CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

**Vulnerability CVE-2022-3586**

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

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

**Vulnerability CVE-2022-4378**

A stack overflow flaw was found in the Linux kernel's SYSCTL subsystem in how a user changes certain kernel parameters and variables. 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-787: Out-of-bounds Write

**Vulnerability CVE-2022-4662**

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

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



**Vulnerability CVE-2022-20421**

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

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

**Vulnerability CVE-2022-20422**

In emulation\_proc\_handler of armv8\_deprecated.c, there is a possible way to corrupt memory due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-237540956 References: Upstream kernel

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

**Vulnerability CVE-2022-21233**

Improper isolation of shared resources in some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.

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

**Vulnerability CVE-2022-23218**

The deprecated compatibility function svcunix\_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its path argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.

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

**Vulnerability CVE-2022-23219**

The deprecated compatibility function clnt\_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its hostname argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.

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

**Vulnerability CVE-2022-28391**

BusyBox through 1.35.0 allows remote attackers to execute arbitrary code if netstat is used to print a DNS PTR record's value to a VT compatible terminal. Alternatively, the attacker could choose to change the terminal's colors.

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/E:P/RL:O/RC:C](#)  
CWE CWE-311: Missing Encryption of Sensitive Data

**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-2022-39188**

An issue was discovered in include/asm-generic/tlb.h in the Linux kernel before 5.19. Because of a race condition (unmap\_mapping\_range versus munmap), a device driver can free a page while it still has stale TLB entries. This only occurs in situations with VM\_PFNMAP VMAs.

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

**Vulnerability CVE-2022-39190**

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

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

**Vulnerability CVE-2022-40307**

An issue was discovered in the Linux kernel through 5.19.8. drivers/firmware/efi/capsule-loader.c has a race condition with a resultant use-after-free.

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

**Vulnerability CVE-2022-41222**

mm/mremap.c in the Linux kernel before 5.13.3 has a use-after-free via a stale TLB because an rmap lock is not held during a PUD move.

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

**Vulnerability CVE-2022-42703**

mm/rmap.c in the Linux kernel before 5.19.7 has a use-after-free related to leaf anon\_vma double reuse.

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

**Vulnerability CVE-2023-0179**

A buffer overflow vulnerability was found in the Netfilter subsystem in the Linux Kernel. This issue could allow the leakage of both stack and heap addresses, and potentially allow Local Privilege Escalation to the root user via arbitrary code execution.

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

**Vulnerability CVE-2023-0394**

A NULL pointer dereference flaw was found in rawv6\_push\_pending\_frames in net/ipv6/raw.c in the network subcomponent in the Linux kernel. This flaw causes the system to crash.

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-311: Missing Encryption of Sensitive Data

**Vulnerability CVE-2023-1073**

A memory corruption flaw was found in the Linux kernel's human interface device (HID) subsystem in how a user inserts a malicious USB device. This flaw allows a local user to crash or potentially escalate their privileges on the system.

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

**Vulnerability CVE-2023-2898**

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

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

**Vulnerability CVE-2023-3390**

A use-after-free vulnerability was found in the Linux kernel's netfilter subsystem in net/netfilter/nf\_tables\_api.c.

Mishandled error handling with NFT\_MSG\_NEWRULE makes it possible to use a dangling pointer in the same transaction causing a use-after-free vulnerability. This flaw allows a local attacker with user access to cause a privilege escalation issue.

We recommend upgrading past commit 1240eb93f0616b21c675416516ff3d74798fdc97.

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

### **Vulnerability CVE-2023-3610**

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

Flaw in the error handling of bound chains causes a use-after-free in the abort path of NFT\_MSG\_NEWRULE. The vulnerability requires CAP\_NET\_ADMIN to be triggered.

CVSS v3.1 Base Score	7.8
CVSS Vector	<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-2023-3611**

An out-of-bounds write vulnerability in the Linux kernel's net/sched: sch\_qfq component can be exploited to achieve local privilege escalation.

The qfq\_change\_agg() function in net/sched/sch\_qfq.c allows an out-of-bounds write because lmax is updated according to packet sizes without bounds checks.

CVSS v3.1 Base Score	7.8
CVSS Vector	<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-2023-3776**

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

If tcf\_change\_indev() fails, fw\_set\_parms() will immediately return an error after incrementing or decrementing the reference counter in tcf\_bind\_filter(). If an attacker can control the reference counter and set it to zero, they can cause the reference to be freed, leading to a use-after-free vulnerability.

CVSS v3.1 Base Score	7.8
CVSS Vector	<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-2023-4004**

A use-after-free flaw was found in the Linux kernel's netfilter in the way a user triggers the nft\_pipapo\_remove function with the element, without a NFT\_SET\_EXT\_KEY\_END. This issue could allow a local user to crash the system or potentially escalate their privileges on the system.

CVSS v3.1 Base Score	7.8
CVSS Vector	<a href="#">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</a>
CWE	CWE-20: Improper Input Validation

### **Vulnerability CVE-2023-4015**

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

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

**Vulnerability CVE-2023-4128**

A use-after-free vulnerability in net/sched/cls\_fw.c in classifiers (cls\_fw, cls\_u32, and cls\_route) in the Linux Kernel allows a local attacker to perform a local privilege escalation due to incorrect handling of the existing filter, leading to a kernel information leak.

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:U/RL:O/RC:C](#)  
CWE CWE-416: Use After Free

**Vulnerability CVE-2023-4147**

A use-after-free vulnerability in the Linux kernel's Netfilter functionality when adding a rule with NFTA\_RULE\_CHAIN\_ID allows a local user to crash or escalate their privileges on the system.

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

**Vulnerability CVE-2023-4273**

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

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

**Vulnerability CVE-2023-4527**

A flaw was found in glibc. When the getaddrinfo function is called with the AF\_UNSPEC address family and the system is configured with no-aaaa mode via /etc/resolv.conf, a DNS response via TCP larger than 2048 bytes can potentially disclose stack contents through the function returned address data, and may cause a crash.

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

**Vulnerability CVE-2023-4806**

A flaw was found in glibc. In an extremely rare situation, the getaddrinfo function may access memory that has been freed, resulting in an application crash. This issue is only exploitable when a NSS module implements only the *nssgethostbyname2\_r* and *\_nssgetcanonname\_r* hooks without implementing the *\_nss\*\_gethostbyname3\_r* hook. The resolved name should return a large number of IPv6 and IPv4, and the call to the getaddrinfo function should have the AF\_INET6 address family with AI\_CANONNAME, AI\_ALL and AI\_V4MAPPED as flags.

CVSS v3.1 Base Score 5.9  
CVSS Vector [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H](#)  
CWE CWE-416: Use After Free

### **Vulnerability CVE-2023-4911**

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

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

### **Vulnerability CVE-2023-5156**

A flaw was found in the GNU C Library. A recent fix for CVE-2023-4806 introduced the potential for a memory leak, which may result in an application crash.

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-401: Missing Release of Memory after Effective Lifetime

### **Vulnerability CVE-2023-31248**

Linux Kernel nftables Use-After-Free Local Privilege Escalation Vulnerability; `nft_chain_lookup_byid` () failed to check whether a chain was active and CAP\_NET\_ADMIN is in any user or network namespace

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

### **Vulnerability CVE-2023-35001**

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

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

### **Vulnerability CVE-2023-45863**

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

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

## **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 (2023-06-13): Publication Date  
V1.1 (2023-09-12): Added CVE-2022-1015, CVE-2023-2898, CVE-2023-31248, CVE-2023-3390, CVE-2023-35001, CVE-2023-3610, CVE-2023-3611, CVE-2023-3776, CVE-2023-4004, CVE-2023-4015, CVE-2023-4128, CVE-2023-4147, CVE-2023-4273  
V1.2 (2023-11-14): Added CVE-2023-4527, CVE-2023-4806, CVE-2023-4911, CVE-2023-5156  
V1.3 (2023-12-12): Added CVE-2021-44879, CVE-2023-45863  
V1.4 (2024-04-09): Added fix for SIMATIC S7-1500 TM MFP - BIOS

## **TERMS OF USE**

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