SSA-337522: Multiple Vulnerabilities in TIM 1531 IRC before V2.4.8

Publication Date:	2024-06-11
Last Update:	2024-07-09
Current Version:	V1.1
CVSS v3.1 Base Score:	9.8
CVSS v4.0 Base Score:	6.9

SUMMARY

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0): All versions < V2.4.8 affected by all CVEs	Update to V2.4.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109954889/
TIM 1531 IRC (6GK7543-1MX00-0XE0): All versions < V2.4.8 affected by all CVEs	Update to V2.4.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109954889/

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

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7, DNP3 and IEC 60870-5-101/104 with three RJ45 interfaces for communication via IP-based networks (WAN / LAN) and a RS 232/RS 485 interface for communication via classic WAN networks.

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-2021-47178

In the Linux kernel, the following vulnerability has been resolved: scsi: target: core: Avoid smp_processor_id() in preemptible code.

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

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-2022-4304

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

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

Vulnerability CVE-2022-4450

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

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

Vulnerability CVE-2022-39189

An issue was discovered the x86 KVM subsystem in the Linux kernel before 5.18.17. Unprivileged guest users can compromise the guest kernel because TLB flush operations are mishandled in certain KVM_VCPU_PREEMPTED situations.

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

Vulnerability CVE-2022-40225

Casting an internal value could lead to floating point exception under certain circumstances. This could allow an attacker to cause a denial of service condition on affected devices.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	6.9
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-681: Incorrect Conversion between Numeric Types

Vulnerability CVE-2022-40303

An issue was discovered in libxml2 before 2.10.3. When parsing a multi-gigabyte XML document with the XML_PARSE_HUGE parser option enabled, several integer counters can overflow. This results in an attempt to access an array at a negative 2GB offset, typically leading to a segmentation fault.

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-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-40304

An issue was discovered in libxml2 before 2.10.3. Certain invalid XML entity definitions can corrupt a hash table key, potentially leading to subsequent logic errors. In one case, a double-free can be provoked.

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-415: Double Free

Vulnerability CVE-2022-45886

An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_net.c has a .disconnect versus dvb_device_open race condition that leads to a use-after-free.

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

Vulnerability CVE-2022-45887

An issue was discovered in the Linux kernel through 6.0.9. drivers/media/usb/ttusb-dec/ttusb_dec.c has a memory leak because of the lack of a dvb_frontend_detach call.

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-2022-45919

An issue was discovered in the Linux kernel through 6.0.10. In drivers/media/dvb-core/dvb_ca_en50221.c, a use-after-free can occur is there is a disconnect after an open, because of the lack of a wait_event.

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

Vulnerability CVE-2023-0160

A deadlock flaw was found in the Linux kernel's BPF subsystem. This flaw allows a local user to potentially 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-667: Improper Locking

Vulnerability CVE-2023-0215

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

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

Vulnerability CVE-2023-0286

There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.

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

Vulnerability CVE-2023-0464

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

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

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

Vulnerability CVE-2023-0465

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

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

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

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

Vulnerability CVE-2023-0466

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

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

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

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

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

Vulnerability CVE-2023-1017

An out-of-bounds write vulnerability exists in TPM2.0's Module Library allowing writing of a 2-byte data past the end of TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can lead to denial of service (crashing the TPM chip/process or rendering it unusable) and/or arbitrary code execution in the TPM context.

CVSS v3.1 Base Score	4.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/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-2023-2124

An out-of-bounds memory access flaw was found in the Linux kernel's XFS file system in how a user restores an XFS image after failure (with a dirty log journal). 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-2023-2269

A denial of service problem was found, due to a possible recursive locking scenario, resulting in a deadlock in table_clear in drivers/md/dm-ioctl.c in the Linux Kernel Device Mapper-Multipathing sub-component.

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/E:P/RL:O/RC:C
CWE	CWE-667: Improper Locking

Vulnerability CVE-2023-21255

In multiple functions of binder.c, there is a possible memory corruption 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.

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-2023-27321

OPC Foundation UA .NET Standard ConditionRefresh Resource Exhaustion Denial-of-Service Vulnerability. This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of OPC Foundation UA .NET Standard. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of OPC UA ConditionRefresh requests. By sending a large number of requests, an attacker can consume all available resources on the server. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-20505.

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-1325: Improperly Controlled Sequential Memory Allocation

Vulnerability CVE-2023-28319

A use after free vulnerability exists in curl <v8.1.0 in the way libcurl offers a feature to verify an SSH server's public key using a SHA 256 hash. When this check fails, libcurl would free the memory for the fingerprint before it returns an error message containing the (now freed) hash. This flaw risks inserting sensitive heap-based data into the error message that might be shown to users or otherwise get leaked and revealed.

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-416: Use After Free

Vulnerability CVE-2023-35788

An issue was discovered in fl_set_geneve_opt in net/sched/cls_flower.c in the Linux kernel before 6.3.7. It allows an out-of-bounds write in the flower classifier code via TCA_FLOWER_KEY_ENC_OPTS_GENEVE packets. This may result in denial of service or 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-787: Out-of-bounds Write

Vulnerability CVE-2023-35823

An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in saa7134_finidev in drivers/media/pci/saa7134/saa7134-core.c.

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

Vulnerability CVE-2023-35824

An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in dm1105_remove in drivers/media/pci/dm1105/dm1105.c.

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

Vulnerability CVE-2023-35828

An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in renesas_usb3_remove in drivers/usb/gadget/udc/renesas_usb3.c.

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

Vulnerability CVE-2023-35829

An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in rkvdec_remove in drivers/staging/media/rkvdec/rkvdec.c.

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

Vulnerability CVE-2023-41910

An issue was discovered in lldpd before 1.0.17. By crafting a CDP PDU packet with specific CDP_TLV_ADDRESSES TLVs, a malicious actor can remotely force the lldpd daemon to perform an out-of-bounds read on heap memory. This occurs in cdp_decode in daemon/protocols/cdp.c.

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-125: Out-of-bounds Read

Vulnerability CVE-2023-50763

The web server of affected products, if configured to allow the import of PKCS12 containers, could end up in an infinite loop when processing incomplete certificate chains.

This could allow an authenticated remote attacker to create a denial of service condition by importing specially crafted PKCS12 containers.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	6.9
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

Vulnerability CVE-2023-52474

In the Linux kernel, the following vulnerability has been resolved: IB/hfi1: Fix bugs with non-PAGE_SIZE-end multi-iovec user SDMA requests hfi1 user SDMA request processing has two bugs that can cause data corruption for user SDMA requests that have multiple payload iovecs where an iovec other than the tail iovec does not run up to the page boundary for the buffer pointed to by that iovec.a Here are the specific bugs: 1. user_sdma_txadd() does not use struct user_sdma_iovec->iov.iov_len. Rather, user_sdma_txadd() will add up to PAGE_SIZE bytes from iovec to the packet, even if some of those bytes are past iovec->iov.iov_len and are thus not intended to be in the packet. 2. user_sdma_txadd() and user_sdma_send_pkts() fail to advance to the next iovec in user_sdma_request->iovs when the current iovec is not PAGE_SIZE and does not contain enough data to complete the packet. The transmitted packet will contain the wrong data from the iovec pages. This has not been an issue with SDMA packets from hfi1 Verbs or PSM2 because they only produce iovecs that end short of PAGE_SIZE as the tail iovec of an SDMA request. Fixing these bugs exposes other bugs with the SDMA pin cache (struct mmu_rb_handler) that get in way of supporting user SDMA requests with multiple payload iovecs whose buffers do not end at PAGE_SIZE. So this commit fixes those issues as well. Here are the mmu_rb_handler bugs that non-PAGE_SIZE-end multi-iovec payload user SDMA requests can hit: 1. Overlapping memory ranges in mmu_rb_handler will result in duplicate pinnings. 2. When extending an existing mmu_rb_handler entry (struct mmu_rb_node), the mmu_rb code (1) removes the existing entry under a lock, (2) releases that lock, pins the new pages, (3) then reacquires the lock to insert the extended mmu_rb_node. If someone else comes in and inserts an overlapping entry between (2) and (3), insert in (3) will fail. The failure path code in this case unpins *all* pages in either the original mmu_rb_node or the new mmu_rb_node that was inserted between (2) and (3). 3. In hfi1_mmu_rb_remove_unless_exact(), mmu_rb_node->refcount is incremented outside of mmu_rb_handler->lock. As a result, mmu_rb_node could be evicted by another thread that gets mmu_rb_handler->lock and checks mmu_rb_node->refcount before mmu_rb_node->refcount is incremented. 4. Related to #2 above, SDMA request submission failure path does not check mmu_rb_node->refcount before freeing mmu_rb_node object. If there are other SDMA requests in progress whose iovecs have pointers to the now-freed mmu_rb_node(s), those pointers to the now-freed mmu_rb nodes will be dereferenced when those SDMA requests complete.

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-2024-0775

A use-after-free flaw was found in the __ext4_remount in fs/ext4/super.c in ext4 in the Linux kernel. This flaw allows a local user to cause an information leak problem while freeing the old quota file names before a potential failure, leading to a use-after-free.

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-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 (2024-06-11):	Publication Date
V1.1 (2024-07-09):	Updated contents of CVE-2023-27321 (OPC Foundation UA .NET Standard: Description, CVSS vector, CWE)

TERMS OF USE

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