SSA-625862: Multiple Vulnerabilities in Third-Party Components in SIMATIC CP 1542SP-1 and CP 1543SP-1 before V2.3

Publication Date:	2024-06-11
Last Update:	2024-06-11
Current Version:	V1.0
CVSS v3.1 Base Score:	9.8
CVSS v4.0 Base Score:	8.7

SUMMARY

SIMATIC CP 1542SP-1 and CP 1543SP-1 before V2.3 are affected by multiple vulnerabilities in third-party components and the integrated web server.

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
SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/
SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/
SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/
SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/
SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/
SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/

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

SIMATIC CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communications processors connect SIMATIC ET 200SP controllers to Ethernet networks. SIMATIC CP 1543SP-1 and CP 1542SP-1 IRC communications processors also provide integrated security functions such as firewall, Virtual Private Networks (VPN) or support other protocols with data encryption.

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-2022-2097

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

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

Vulnerability CVE-2022-3435

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-2022-3545

A vulnerability has been found in Linux Kernel and classified as critical. Affected by this vulnerability is the function area_cache_get of the file drivers/net/ethernet/netronome/nfp/nfpcore/nfp_cppcore.c of the component IPsec. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier VDB-211045 was assigned to this vulnerability.

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

Vulnerability CVE-2022-3623

A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function follow_page_pte of the file mm/gup.c of the component BPF. The manipulation leads to race condition. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211921 was assigned to this vulnerability.

CVSS v3.1 Base Score	5.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2022-3643

Guests can trigger NIC interface reset/abort/crash via netback It is possible for a guest to trigger a NIC interface reset/abort/crash in a Linux based network backend by sending certain kinds of packets. It appears to be an (unwritten?) assumption in the rest of the Linux network stack that packet protocol headers are all contained within the linear section of the SKB and some NICs behave badly if this is not the case. This has been reported to occur with Cisco (enic) and Broadcom NetXtrem II BCM5780 (bnx2x) though it may be an issue with other NICs/drivers as well. In case the frontend is sending requests with split headers, netback will forward those violating above mentioned assumption to the networking core, resulting in said misbehavior.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

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-2022-40303

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-2022-42328

Guests can trigger deadlock in Linux netback driver [This CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] The patch for XSA-392 introduced another issue which might result in a deadlock when trying to free the SKB of a packet dropped due to the XSA-392 handling (CVE-2022-42328). Additionally when dropping packages for other reasons the same deadlock could occur in case of netpoll being active for the interface the xen-netback driver is connected to (CVE-2022-42329).

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

Vulnerability CVE-2022-42329

Guests can trigger deadlock in Linux netback drive. The patch for XSA-392 introduced another issue which might result in a deadlock when trying to free the SKB of a packet dropped due to the XSA-392 handling (CVE-2022-42328). Additionally when dropping packages for other reasons the same deadlock could occur in case of netpoll being active for the interface the xen-netback driver is connected to (CVE-2022-42329).

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

Vulnerability CVE-2022-44792

handle_ipDefaultTTL in agent/mibgroup/ip-mib/ip_scalars.c in Net-SNMP 5.8 through 5.9.3 has a NULL Pointer Exception bug that can be used by a remote attacker (who has write access) to cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.

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-476: NULL Pointer Dereference

Vulnerability CVE-2022-44793

handle_ipv6IpForwarding in agent/mibgroup/ip-mib/ip_scalars.c in Net-SNMP 5.4.3 through 5.9.3 has a NULL Pointer Exception bug that can be used by a remote attacker to cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.

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-476: NULL Pointer Dereference

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-2023-28484

In libxml2 before 2.10.4, parsing of certain invalid XSD schemas can lead to a NULL pointer dereference and subsequently a segfault. This occurs in xmlSchemaFixupComplexType in xmlschemas.c.

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-476: NULL Pointer Dereference

Vulnerability CVE-2023-29469

An issue was discovered in libxml2 before 2.10.4. When hashing empty dict strings in a crafted XML document, xmlDictComputeFastKey in dict.c can produce non-deterministic values, leading to various logic and memory errors, such as a double free. This behavior occurs because there is an attempt to use the first byte of an empty string, and any value is possible (not solely the '\0' value).

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-415: Double Free

Vulnerability CVE-2023-38380

The webserver implementation of the affected products does not correctly release allocated memory after it has been used.

An attacker with network access could use this vulnerability to cause a denial-of-service condition in the webserver of the affected product.

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-401: Missing Release of Memory after Effective Lifetime

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')

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

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.