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

Publication Date: 2024-04-09
Last Update: 2024-07-09
Current Version: V1.2
CVSS v3.1 Base Score: 7.8

SUMMARY

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

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

AFFECTED PRODUCTS AND SOLUTION

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

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Only build and run applications from trusted sources

Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

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

PRODUCT DESCRIPTION

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

VULNERABILITY DESCRIPTION

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

Vulnerability CVE-2023-5678

Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2023-6121

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

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-6817

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

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

We recommend upgrading past commit 317eb9685095678f2c9f5a8189de698c5354316a.

CVSS v3.1 Base Score	7.8
CVSS Vector	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-2023-6931

A heap out-of-bounds write vulnerability in the Linux kernel's Performance Events system component can be exploited to achieve local privilege escalation.

A perf_event's read_size can overflow, leading to an heap out-of-bounds increment or write in perf_read_group().

We recommend upgrading past commit 382c27f4ed28f803b1f1473ac2d8db0afc795a1b.

CVSS v3.1 Base Score	7.8
CVSS Vector	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-2023-6932

A use-after-free vulnerability in the Linux kernel's ipv4: igmp component can be exploited to achieve local privilege escalation.

A race condition can be exploited to cause a timer be mistakenly registered on a RCU read locked object which is freed by another thread.

We recommend upgrading past commit e2b706c691905fe78468c361aaabc719d0a496f1.

CVSS v3.1 Base Score	7.8
CVSS Vector	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-2023-45898

The Linux kernel before 6.5.4 has an es1 use-after-free in fs/ext4/extents_status.c, related to ext4_es_insert_extent.

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

Vulnerability CVE-2024-0584

A use-after-free issue was found in igmp_start_timer in net/ipv4/igmp.c in the network sub-component in the Linux Kernel. This flaw allows a local user to observe a refcnt use-after-free issue when receiving an igmp query packet, leading to a kernel information leak.

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

Vulnerability CVE-2024-0727

Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack

Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly.

A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue.

OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass().

We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant.

The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

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

Vulnerability CVE-2024-2511

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

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2024-5535

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

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

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2024-04-09): Publication Date
V1.1 (2024-05-14): Added CVE-2024-2511
V1.2 (2024-07-09): Added CVE-2024-5535

TERMS OF USE