

SSA-879734: Multiple Vulnerabilities in SCALANCE XM-400/XR-500 before V6.6.1

Publication Date: 2024-06-11
Last Update: 2024-06-11
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

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
SCALANCE XM408-4C (6GK5408-4GP00-2AM2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XM408-4C (L3 int.) (6GK5408-4GQ00-2AM2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XM408-8C (6GK5408-8GS00-2AM2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XM408-8C (L3 int.) (6GK5408-8GR00-2AM2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XM416-4C (6GK5416-4GS00-2AM2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XM416-4C (L3 int.) (6GK5416-4GR00-2AM2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR524-8C, 1x230V (6GK5524-8GS00-3AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR524-8C, 1x230V (L3 int.) (6GK5524-8GR00-3AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/

SCALANCE XR524-8C, 2x230V (6GK5524-8GS00-4AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR524-8C, 2x230V (L3 int.) (6GK5524-8GR00-4AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR524-8C, 24V (6GK5524-8GS00-2AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR524-8C, 24V (L3 int.) (6GK5524-8GR00-2AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR526-8C, 1x230V (6GK5526-8GS00-3AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR526-8C, 1x230V (L3 int.) (6GK5526-8GR00-3AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR526-8C, 2x230V (6GK5526-8GS00-4AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR526-8C, 2x230V (L3 int.) (6GK5526-8GR00-4AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR526-8C, 24V (6GK5526-8GS00-2AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR526-8C, 24V (L3 int.) (6GK5526-8GR00-2AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR528-6M (2HR2) (6GK5528-0AA00-2HR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR528-6M (2HR2, L3 int.) (6GK5528-0AR00-2HR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/

SCALANCE XR528-6M (6GK5528-0AA00-2AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR528-6M (L3 int.) (6GK5528-0AR00-2AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR552-12M (2HR2) (6GK5552-0AA00-2HR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR552-12M (2HR2) (6GK5552-0AR00-2HR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR552-12M (2HR2, L3 int.) (6GK5552-0AR00-2AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/
SCALANCE XR552-12M (6GK5552-0AA00-2AR2): All versions < V6.6.1 affected by all CVEs	Update to V6.6.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109955252/

WORKAROUNDS AND MITIGATIONS

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

GENERAL SECURITY RECOMMENDATIONS

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

PRODUCT DESCRIPTION

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

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-2022-4304

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-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

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.