SSA-699386: Multiple Vulnerabilities in SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family before V4.5

Publication Date: 2023-11-14
Last Update: 2023-12-12
Current Version: V1.1
CVSS v3.1 Base Score: 9.1

SUMMARY

SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG Family before V4.5 is affected by multiple vulnerabilities.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE XB205-3 (SC, PN) (6GK5205-3BB00-2AB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BB00-2TB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BD00-2TB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB205-3 (ST, PN) (6GK5205-3BD00-2AB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB205-3LD (SC, E/IP) (6GK5205-3BF00-2TB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB205-3LD (SC, PN) (6GK5205-3BF00-2AB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB208 (E/IP) (6GK5208-0BA00-2TB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB208 (PN) (6GK5208-0BA00-2AB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/

SCALANCE XB213-3 (SC, E/IP) (6GK5213-3BD00-2TB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB213-3 (SC, PN) (6GK5213-3BD00-2AB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB213-3 (ST, E/IP) (6GK5213-3BB00-2TB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB213-3 (ST, PN) (6GK5213-3BB00-2AB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB213-3LD (SC, E/IP) (6GK5213-3BF00-2TB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB213-3LD (SC, PN) (6GK5213-3BF00-2AB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB216 (E/IP) (6GK5216-0BA00-2TB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XB216 (PN) (6GK5216-0BA00-2AB2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC206-2 (SC) (6GK5206-2BD00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC206-2 (ST/BFOC) (6GK5206-2BB00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC206-2G PoE (6GK5206-2RS00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC206-2G PoE (54 V DC) (6GK5206-2RS00-5AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/

SCALANCE XC206-2G PoE EEC (54 V DC) (6GK5206-2RS00-5FC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC206-2SFP (6GK5206-2BS00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC206-2SFP EEC (6GK5206-2BS00-2FC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC206-2SFP G (6GK5206-2GS00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC206-2SFP G (EIP DEF.) (6GK5206-2GS00-2TC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC206-2SFP G EEC (6GK5206-2GS00-2FC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC208 (6GK5208-0BA00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC208EEC (6GK5208-0BA00-2FC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC208G (6GK5208-0GA00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC208G (EIP def.) (6GK5208-0GA00-2TC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC208G EEC (6GK5208-0GA00-2FC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC208G PoE (6GK5208-0RA00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/

SCALANCE XC208G PoE (54 V DC) (6GK5208-0RA00-5AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC216 (6GK5216-0BA00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC216-3G PoE (6GK5216-3RS00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC216-3G PoE (54 V DC) (6GK5216-3RS00-5AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC216-4C (6GK5216-4BS00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC216-4C G (6GK5216-4GS00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC216-4C G (EIP Def.) (6GK5216-4GS00-2TC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC216-4C G EEC (6GK5216-4GS00-2FC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC216EEC (6GK5216-0BA00-2FC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC224 (6GK5224-0BA00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC224-4C G (6GK5224-4GS00-2AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XC224-4C G (EIP Def.) (6GK5224-4GS00-2TC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/

SCALANCE XC224-4C G EEC (6GK5224-4GS00-2FC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XF204 (6GK5204-0BA00-2GF2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XF204 DNA (6GK5204-0BA00-2YF2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XF204-2BA (6GK5204-2AA00-2GF2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XF204-2BA DNA (6GK5204-2AA00-2YF2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XP208 (6GK5208-0HA00-2AS6): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XP208 (Ethernet/IP) (6GK5208-0HA00-2TS6): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XP208EEC (6GK5208-0HA00-2ES6): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XP208PoE EEC (6GK5208-0UA00-5ES6): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XP216 (6GK5216-0HA00-2AS6): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XP216 (Ethernet/IP) (6GK5216-0HA00-2TS6): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XP216EEC (6GK5216-0HA00-2ES6): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/

SCALANCE XP216POE EEC (6GK5216-0UA00-5ES6): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XR324WG (24 x FE, AC 230V) (6GK5324-0BA00-3AR3): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XR324WG (24 X FE, DC 24V) (6GK5324-0BA00-2AR3): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XR326-2C PoE WG (6GK5326-2QS00-3AR3): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XR326-2C PoE WG (without UL) (6GK5326-2QS00-3RR3): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3AR3): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3RR3): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XR328-4C WG (24XFE, 4XGE, 24V) (6GK5328-4FS00-2AR3): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XR328-4C WG (24xFE, 4xGE,DC24V) (6GK5328-4FS00-2RR3): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XR328-4C WG (28xGE, AC 230V) (6GK5328-4SS00-3AR3): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SCALANCE XR328-4C WG (28xGE, DC 24V) (6GK5328-4SS00-2AR3): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SIPLUS NET SCALANCE XC206-2 (6AG1206-2BB00-7AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/

SIPLUS NET SCALANCE XC206-2SFP (6AG1206-2BS00-7AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SIPLUS NET SCALANCE XC208 (6AG1208-0BA00-7AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/
SIPLUS NET SCALANCE XC216-4C (6AG1216-4BS00-7AC2): All versions < V4.5	Update to V4.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109825818/

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 W products are wireless communication devices used to connect industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs), according to the IEEE 802.11 standard (802.11ac, 802.11a/b/g/h, and/or 802.11n).

SCALANCE W-1700 products are wireless communication devices based on IEEE 802.11ac standard. They are used to connect all to sorts of WLAN devices (Access Points or Clients, depending on the operating mode) with a strong focus on industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs) and others.

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

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2022-4203

A read buffer overrun can be triggered in X.509 certificate verification, specifically in name constraint checking. Note that this occurs after certificate chain signature verification and requires either a CA to have signed the malicious certificate or for the application to continue certificate verification despite failure to construct a path to a trusted issuer. The read buffer overrun might result in a crash which could lead to a denial of service attack. In theory it could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext) although we are not aware of any working exploit leading to memory contents disclosure as of the time of release of this advisory. In a TLS client, this can be triggered by connecting to a malicious server. In a TLS server, this can be triggered if the server requests client authentication and a malicious client connects.

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
CWE	CWE-125: Out-of-bounds Read

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:U/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:U/RL:O/RC:C
CWE	CWE-415: Double Free

Vulnerability CVE-2023-0216

An invalid pointer dereference on read can be triggered when an application tries to load malformed PKCS7 data with the d2i_PKCS7(), d2i_PKCS7_bio() or d2i_PKCS7_fp() functions. The result of the dereference is an application crash which could lead to a denial of service attack. The TLS implementation in OpenSSL does not call this function however third party applications might call these functions on untrusted 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-476: NULL Pointer Dereference

Vulnerability CVE-2023-0217

An invalid pointer dereference on read can be triggered when an application tries to check a malformed DSA public key by the EVP_PKEY_public_check() function. This will most likely lead to an application crash. This function can be called on public keys supplied from untrusted sources which could allow an attacker to cause a denial of service attack. The TLS implementation in OpenSSL does not call this function but applications might call the function if there are additional security requirements imposed by standards such as FIPS 140-3.

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-2023-0401

A NULL pointer can be dereferenced when signatures are being verified on PKCS7 signed or signedAndEnveloped data. In case the hash algorithm used for the signature is known to the OpenSSL library but the implementation of the hash algorithm is not available the digest initialization will fail. There is a missing check for the return value from the initialization function which later leads to invalid usage of the digest API most likely leading to a crash. The unavailability of an algorithm can be caused by using FIPS enabled configuration of providers or more commonly by not loading the legacy provider. PKCS7 data is processed by the SMIME library calls and also by the time stamp (TS) library calls. The TLS implementation in OpenSSL does not call these functions however third party applications would be affected if they call these functions to verify signatures on untrusted 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-476: NULL Pointer Dereference

Vulnerability CVE-2023-2650

Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that use OBJ_obj2txt() directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit may experience notable to very long delays when processing those messages, which may lead to a Denial of Service. An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers - most of which have no size limit. OBJ_obj2txt() may be used to translate an ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSL type ASN1_OBJECT) to its canonical numeric text form, which are the sub-identifiers of the OBJECT IDENTIFIER in decimal form, separated by periods. When one of the sub-identifiers in the OBJECT IDENTIFIER is very large (these are sizes that are seen as absurdly large, taking up tens or hundreds of KiBs), the translation to a decimal number in text may take a very long time. The time complexity is O(square(n)) with 'n' being the size of the sub-identifiers in bytes (*). With OpenSSL 3.0, support to fetch cryptographic algorithms using names / identifiers in string form was introduced. This includes using OBJECT IDENTIFIERs in canonical numeric text form as identifiers for fetching algorithms. Such OBJECT IDENTIFIERs may be received through the ASN.1 structure AlgorithmIdentifier, which is commonly used in multiple protocols to specify what cryptographic algorithm should be used to sign or verify, encrypt or decrypt, or digest passed data. Applications that call OBJ_obj2txt() directly with untrusted data are affected, with any version of OpenSSL. If the use is for the mere purpose of display, the severity is considered low. In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS. It also impacts anything that processes X.509 certificates, including simple things like verifying its signature. The impact on TLS is relatively low, because all versions of OpenSSL have a 100KiB limit on the peer's certificate chain. Additionally, this only impacts clients, or servers that have explicitly enabled client authentication. In OpenSSL 1.1.1 and 1.0.2, this only affects displaying diverse objects, such as X.509 certificates. This is assumed to not happen in such a way that it would cause a Denial of Service, so these versions are considered not affected by this issue in such a way that it would be cause for concern, and the severity is therefore considered low.

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-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2023-44317

Affected products do not properly validate the content of uploaded X509 certificates which could allow an attacker with administrative privileges to execute arbitrary code on the device.

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data

Vulnerability CVE-2023-44318

Affected devices use a hardcoded key to obfuscate the configuration backup that an administrator can export from the device. This could allow an authenticated attacker with administrative privileges or an attacker that obtains a configuration backup to extract configuration information from the exported file.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-321: Use of Hard-coded Cryptographic Key

Vulnerability CVE-2023-44319

Affected devices use a weak checksum algorithm to protect the configuration backup that an administrator can export from the device. This could allow an authenticated attacker with administrative privileges or an attacker that tricks a legitimate administrator to upload a modified configuration file to change the configuration of an affected device.

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:H/A:N/E:P/RL:O/RC:C
CWE	CWE-328: Use of Weak Hash

Vulnerability CVE-2023-44320

Affected devices do not properly validate the authentication when performing certain modifications in the web interface allowing an authenticated attacker to influence the user interface configured by an administrator.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-425: Direct Request ('Forced Browsing')

Vulnerability CVE-2023-44321

Affected devices do not properly validate the length of inputs when performing certain configuration changes in the web interface allowing an authenticated attacker to cause a denial of service condition. The device needs to be restarted for the web interface to become available again.

CVSS v3.1 Base Score	2.7
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2023-44322

Affected devices can be configured to send emails when certain events occur on the device. When presented with an invalid response from the SMTP server, the device triggers an error that disrupts email sending. An attacker with access to the network can use this to do disable notification of users when certain events occur.

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-252: Unchecked Return Value

Vulnerability CVE-2023-44373

Affected devices do not properly sanitize an input field. This could allow an authenticated remote attacker with administrative privileges to inject code or spawn a system root shell. Follow-up of CVE-2022-36323.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/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-2023-44374

Affected devices allow to change the password, but insufficiently check which password is to be changed. With this an authenticated attacker could, under certain conditions, be able to change the password of another, potential admin user allowing her to escalate her privileges.

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:H/A:N/E:P/RL:O/RC:C
CWE	CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context

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 (2023-11-14): Publication Date
V1.1 (2023-12-12): Clarify: Remove product description for SCALANCE M-800/S615

TERMS OF USE