SSA-813746: BadAlloc Vulnerabilities in SCALANCE X-200, X-200IRT, and X-300 Switch Families

Publication Date: 2023-04-11
Last Update: 2023-04-11
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Siemens has released a new firmware version for SCALANCE X-200 and X-200 IRT switches that address Bad Alloc vulnerabilities in the underlying operating system and recommends to update to the latest versions. Siemens recommends countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE X200-4P IRT (6GK5200-4AH00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X201-3P IRT (6GK5201-3BH00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X201-3P IRT PRO (6GK5201-3JR00-2BA6): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X202-2IRT (6GK5202-2BB00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X202-2IRT (6GK5202-2BB10-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X202-2P IRT (6GK5202-2BH00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X202-2P IRT PRO (6GK5202-2JR00-2BA6): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X204-2 (6GK5204-2BB10-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/

SCALANCE X204-2FM (6GK5204-2BB11-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE X204-2LD (6GK5204-2BC10-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE X204-2LD TS (6GK5204-2BC10-2CA2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE X204-2TS (6GK5204-2BB10-2CA2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE X204IRT (6GK5204-0BA00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X204IRT (6GK5204-0BA10-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X204IRT PRO (6GK5204-0JA00-2BA6): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE X206-1 (6GK5206-1BB10-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE X206-1LD (6GK5206-1BC10-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE X208 (6GK5208-0BA10-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE X208PRO (6GK5208-0HA10-2AA6): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE X212-2 (6GK5212-2BB00-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/

SCALANCE X212-2LD (6GK5212-2BC00-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE X216 (6GK5216-0BA00-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE X224 (6GK5224-0BA00-2AA3): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE X302-7 EEC (2x 24V) (6GK5302-7GD00-2EA3): All versions	Currently no fix is planned
SCALANCE X302-7 EEC (2x 24V, coated) (6GK5302-7GD00-2GA3): All versions	Currently no fix is planned
SCALANCE X302-7 EEC (2x 230V) (6GK5302-7GD00-4EA3): All versions	Currently no fix is planned
SCALANCE X302-7 EEC (2x 230V, coated) (6GK5302-7GD00-4GA3): All versions	Currently no fix is planned
SCALANCE X302-7 EEC (24V) (6GK5302-7GD00-1EA3): All versions	Currently no fix is planned
SCALANCE X302-7 EEC (24V, coated) (6GK5302-7GD00-1GA3): All versions	Currently no fix is planned
SCALANCE X302-7 EEC (230V) (6GK5302-7GD00-3EA3): All versions	Currently no fix is planned
SCALANCE X302-7 EEC (230V, coated) (6GK5302-7GD00-3GA3): All versions	Currently no fix is planned
SCALANCE X304-2FE (6GK5304-2BD00-2AA3): All versions	Currently no fix is planned
SCALANCE X306-1LD FE (6GK5306-1BF00-2AA3): All versions	Currently no fix is planned

SCALANCE X307-2 EEC (2x 24V) (6GK5307-2FD00-2EA3): All versions	Currently no fix is planned
SCALANCE X307-2 EEC (2x 24V, coated) (6GK5307-2FD00-2GA3): All versions	Currently no fix is planned
SCALANCE X307-2 EEC (2x 230V) (6GK5307-2FD00-4EA3): All versions	Currently no fix is planned
SCALANCE X307-2 EEC (2x 230V, coated) (6GK5307-2FD00-4GA3): All versions	Currently no fix is planned
SCALANCE X307-2 EEC (24V) (6GK5307-2FD00-1EA3): All versions	Currently no fix is planned
SCALANCE X307-2 EEC (24V, coated) (6GK5307-2FD00-1GA3): All versions	Currently no fix is planned
SCALANCE X307-2 EEC (230V) (6GK5307-2FD00-3EA3): All versions	Currently no fix is planned
SCALANCE X307-2 EEC (230V, coated) (6GK5307-2FD00-3GA3): All versions	Currently no fix is planned
SCALANCE X307-3 (6GK5307-3BL00-2AA3): All versions	Currently no fix is planned
SCALANCE X307-3 (6GK5307-3BL10-2AA3): All versions	Currently no fix is planned
SCALANCE X307-3LD (6GK5307-3BM00-2AA3): All versions	Currently no fix is planned
SCALANCE X307-3LD (6GK5307-3BM10-2AA3): All versions	Currently no fix is planned
SCALANCE X308-2 (6GK5308-2FL00-2AA3): All versions	Currently no fix is planned
SCALANCE X308-2 (6GK5308-2FL10-2AA3): All versions	Currently no fix is planned
SCALANCE X308-2LD (6GK5308-2FM00-2AA3): All versions	Currently no fix is planned

SCALANCE X308-2LD (6GK5308-2FM10-2AA3): All versions	Currently no fix is planned
SCALANCE X308-2LH (6GK5308-2FN00-2AA3): All versions	Currently no fix is planned
SCALANCE X308-2LH (6GK5308-2FN10-2AA3): All versions	Currently no fix is planned
SCALANCE X308-2LH+ (6GK5308-2FP00-2AA3): All versions	Currently no fix is planned
SCALANCE X308-2LH+ (6GK5308-2FP10-2AA3): All versions	Currently no fix is planned
SCALANCE X308-2M (6GK5308-2GG00-2AA2): All versions	Currently no fix is planned
SCALANCE X308-2M (6GK5308-2GG10-2AA2): All versions	Currently no fix is planned
SCALANCE X308-2M PoE (6GK5308-2QG00-2AA2): All versions	Currently no fix is planned
SCALANCE X308-2M PoE (6GK5308-2QG10-2AA2): All versions	Currently no fix is planned
SCALANCE X308-2M TS (6GK5308-2GG00-2CA2): All versions	Currently no fix is planned
SCALANCE X308-2M TS (6GK5308-2GG10-2CA2): All versions	Currently no fix is planned
SCALANCE X310 (6GK5310-0FA00-2AA3): All versions	Currently no fix is planned
SCALANCE X310 (6GK5310-0FA10-2AA3): All versions	Currently no fix is planned
SCALANCE X310FE (6GK5310-0BA00-2AA3): All versions	Currently no fix is planned
SCALANCE X310FE (6GK5310-0BA10-2AA3): All versions	Currently no fix is planned

SCALANCE X320-1 FE (6GK5320-1BD00-2AA3): All versions	Currently no fix is planned
SCALANCE X320-1-2LD FE (6GK5320-3BF00-2AA3): All versions	Currently no fix is planned
SCALANCE X408-2 (6GK5408-2FD00-2AA2): All versions	Currently no fix is planned
SCALANCE XF201-3P IRT (6GK5201-3BH00-2BD2): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE XF202-2P IRT (6GK5202-2BH00-2BD2): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE XF204 (6GK5204-0BA00-2AF2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE XF204-2 (6GK5204-2BC00-2AF2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE XF204-2BA IRT (6GK5204-2AA00-2BD2): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE XF204IRT (6GK5204-0BA00-2BF2): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SCALANCE XF206-1 (6GK5206-1BC00-2AF2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE XF208 (6GK5208-0BA00-2AF2): All versions < V5.2.6	Update to V5.2.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109811753/
SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG00-2ER2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG10-2ER2): All versions	Currently no fix is planned

SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG00-2JR2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG10-2JR2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-4ER2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-4ER2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-4JR2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-4JR2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG00-1ER2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG10-1ER2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG00-1JR2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG10-1JR2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-3ER2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-3ER2): All versions	Currently no fix is planned

SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-3JR2): All versions	Currently no fix is planned
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-3JR2): All versions	Currently no fix is planned
SCALANCE XR324-4M PoE (24V, ports on front) (6GK5324-4QG00-1AR2): All versions	Currently no fix is planned
SCALANCE XR324-4M PoE (24V, ports on rear) (6GK5324-4QG00-1HR2): All versions	Currently no fix is planned
SCALANCE XR324-4M PoE (230V, ports on front) (6GK5324-4QG00-3AR2): All versions	Currently no fix is planned
SCALANCE XR324-4M PoE (230V, ports on rear) (6GK5324-4QG00-3HR2): All versions	Currently no fix is planned
SCALANCE XR324-4M PoE TS (24V, ports on front) (6GK5324-4QG00-1CR2): All versions	Currently no fix is planned
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG00-1AR2): All versions	Currently no fix is planned
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG10-1AR2): All versions	Currently no fix is planned
SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG00-1HR2): All versions	Currently no fix is planned
SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG10-1HR2): All versions	Currently no fix is planned
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG00-3AR2): All versions	Currently no fix is planned
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG10-3AR2): All versions	Currently no fix is planned

SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG00-3HR2): All versions	Currently no fix is planned
SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG10-3HR2): All versions	Currently no fix is planned
SCALANCE XR324-12M TS (24V) (6GK5324-0GG00-1CR2): All versions	Currently no fix is planned
SCALANCE XR324-12M TS (24V) (6GK5324-0GG10-1CR2): All versions	Currently no fix is planned
SIPLUS NET SCALANCE X202-2P IRT (6AG1202-2BH00-2BA3): All versions < V5.5.2	Update to V5.5.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817790/
SIPLUS NET SCALANCE X308-2 (6AG1308-2FL10-4AA3): All versions	Currently no fix is planned

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).

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.

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-2020-28895

In Wind River VxWorks, memory allocator has a possible overflow in calculating the memory block's size to be allocated by calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2020-35198

An issue was discovered in Wind River VxWorks. The memory allocator has a possible integer overflow in calculating a memory block's size to be allocated by calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.

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-190: Integer Overflow or Wraparound

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 (2023-04-11): Publication Date

TERMS OF USE