SSA-353002: Multiple Vulnerabilities in SCALANCE XB-200 / XC-200 / XP-200 / XF-200BA / XR-300WG Family

Publication Date: 2024-03-12
Last Update: 2024-03-12
Current Version: V1.0
CVSS v3.1 Base Score: 4.9
CVSS v4.0 Base Score: 5.1

SUMMARY

SCALANCE XB-200/XC-200/XP-200/XF-200BA/XR-300WG Family is affected by multiple vulnerabilities. CVE-2023-44318 and CVE-2023-44321 were previously published as part of SSA-699386.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE XB205-3 (SC, PN) (6GK5205-3BB00-2AB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BB00-2TB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB205-3 (ST, E/IP) (6GK5205-3BD00-2TB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB205-3 (ST, PN) (6GK5205-3BD00-2AB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB205-3LD (SC, E/IP) (6GK5205-3BF00-2TB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB205-3LD (SC, PN) (6GK5205-3BF00-2AB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB208 (E/IP) (6GK5208-0BA00-2TB2): All versions affected by all CVEs	Currently no fix is available

SCALANCE XB208 (PN) (6GK5208-0BA00-2AB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB213-3 (SC, E/IP) (6GK5213-3BD00-2TB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB213-3 (SC, PN) (6GK5213-3BD00-2AB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB213-3 (ST, E/IP) (6GK5213-3BB00-2TB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB213-3 (ST, PN) (6GK5213-3BB00-2AB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB213-3LD (SC, E/IP) (6GK5213-3BF00-2TB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB213-3LD (SC, PN) (6GK5213-3BF00-2AB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB216 (E/IP) (6GK5216-0BA00-2TB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XB216 (PN) (6GK5216-0BA00-2AB2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC206-2 (SC) (6GK5206-2BD00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC206-2 (ST/BFOC) (6GK5206-2BB00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC206-2G PoE (6GK5206-2RS00-2AC2): All versions affected by all CVEs	Currently no fix is available

SCALANCE XC206-2G PoE (54 V DC) (6GK5206-2RS00-5AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC206-2G PoE EEC (54 V DC) (6GK5206-2RS00-5FC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC206-2SFP (6GK5206-2BS00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC206-2SFP EEC (6GK5206-2BS00-2FC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC206-2SFP G (6GK5206-2GS00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC206-2SFP G (EIP DEF.) (6GK5206-2GS00-2TC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC206-2SFP G EEC (6GK5206-2GS00-2FC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC208 (6GK5208-0BA00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC208EEC (6GK5208-0BA00-2FC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC208G (6GK5208-0GA00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC208G (EIP def.) (6GK5208-0GA00-2TC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC208G EEC (6GK5208-0GA00-2FC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC208G PoE (6GK5208-0RA00-2AC2): All versions affected by all CVEs	Currently no fix is available

SCALANCE XC208G PoE (54 V DC) (6GK5208-0RA00-5AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC216 (6GK5216-0BA00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC216-3G PoE (6GK5216-3RS00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC216-3G PoE (54 V DC) (6GK5216-3RS00-5AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC216-4C (6GK5216-4BS00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC216-4C G (6GK5216-4GS00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC216-4C G (EIP Def.) (6GK5216-4GS00-2TC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC216-4C G EEC (6GK5216-4GS00-2FC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC216EEC (6GK5216-0BA00-2FC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC224 (6GK5224-0BA00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC224-4C G (6GK5224-4GS00-2AC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC224-4C G (EIP Def.) (6GK5224-4GS00-2TC2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XC224-4C G EEC (6GK5224-4GS00-2FC2): All versions affected by all CVEs	Currently no fix is available

SCALANCE XF204 (6GK5204-0BA00-2GF2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XF204 DNA (6GK5204-0BA00-2YF2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XF204-2BA (6GK5204-2AA00-2GF2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XF204-2BA DNA (6GK5204-2AA00-2YF2): All versions affected by all CVEs	Currently no fix is available
SCALANCE XP208 (6GK5208-0HA00-2AS6): All versions affected by all CVEs	Currently no fix is available
SCALANCE XP208 (Ethernet/IP) (6GK5208-0HA00-2TS6): All versions affected by all CVEs	Currently no fix is available
SCALANCE XP208EEC (6GK5208-0HA00-2ES6): All versions affected by all CVEs	Currently no fix is available
SCALANCE XP208PoE EEC (6GK5208-0UA00-5ES6): All versions affected by all CVEs	Currently no fix is available
SCALANCE XP216 (6GK5216-0HA00-2AS6): All versions affected by all CVEs	Currently no fix is available
SCALANCE XP216 (Ethernet/IP) (6GK5216-0HA00-2TS6): All versions affected by all CVEs	Currently no fix is available
SCALANCE XP216EEC (6GK5216-0HA00-2ES6): All versions affected by all CVEs	Currently no fix is available
SCALANCE XP216POE EEC (6GK5216-0UA00-5ES6): All versions affected by all CVEs	Currently no fix is available
SCALANCE XR324WG (24 x FE, AC 230V) (6GK5324-0BA00-3AR3): All versions affected by all CVEs	Currently no fix is available

SCALANCE XR324WG (24 X FE, DC 24V) (6GK5324-0BA00-2AR3): All versions affected by all CVEs	Currently no fix is available
SCALANCE XR326-2C PoE WG (6GK5326-2QS00-3AR3): All versions affected by all CVEs	Currently no fix is available
SCALANCE XR326-2C PoE WG (without UL) (6GK5326-2QS00-3RR3): All versions affected by all CVEs	Currently no fix is available
SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3AR3): All versions affected by all CVEs	Currently no fix is available
SCALANCE XR328-4C WG (24xFE,4xGE,AC230V) (6GK5328-4FS00-3RR3): All versions affected by all CVEs	Currently no fix is available
SCALANCE XR328-4C WG (24XFE, 4XGE, 24V) (6GK5328-4FS00-2AR3): All versions affected by all CVEs	Currently no fix is available
SCALANCE XR328-4C WG (24xFE, 4xGE,DC24V) (6GK5328-4FS00-2RR3): All versions affected by all CVEs	Currently no fix is available
SCALANCE XR328-4C WG (28xGE, AC 230V) (6GK5328-4SS00-3AR3): All versions affected by all CVEs	Currently no fix is available
SCALANCE XR328-4C WG (28xGE, DC 24V) (6GK5328-4SS00-2AR3): All versions affected by all CVEs	Currently no fix is available
SIPLUS NET SCALANCE XC206-2 (6AG1206-2BB00-7AC2): All versions affected by all CVEs	Currently no fix is available
SIPLUS NET SCALANCE XC206-2SFP (6AG1206-2BS00-7AC2): All versions affected by all CVEs	Currently no fix is available
SIPLUS NET SCALANCE XC208 (6AG1208-0BA00-7AC2): All versions affected by all CVEs	Currently no fix is available

SIPLUS NET SCALANCE XC216-4C (6AG1216-4BS00-7AC2): All versions affected by all CVEs	Currently no fix is available

WORKAROUNDS AND MITIGATIONS

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-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-2023-44321

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
CVSS v4.0 Base Score	5.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-400: Uncontrolled Resource Consumption

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 (2024-03-12): Publication Date

TERMS OF USE