SSA-443566: Authentication Bypass in SCALANCE X Switches Families

Publication Date: 2020-01-14
Last Update: 2022-12-13
Current Version: V1.3
CVSS v3.1 Base Score: 8.8

SUMMARY

Several SCALANCE X switches are affected by an Authentication Bypass vulnerability. The vulnerability allows an unauthenticated attacker to violate access-control rules. The vulnerability can be exploited by sending a GET request to a specific uniform resource locator on the web configuration interface of the device.

The security vulnerability could be exploited by an attacker with network access to the affected systems. An attacker could use the vulnerability to obtain sensitive information or change the device configuration.

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 X204RNA (HSR) (6GK5204-0BA00-2MB2): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA (PRP) (6GK5204-0BA00-2KB2): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA EEC (HSR) (6GK5204-0BS00-2NA3): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA EEC (PRP) (6GK5204-0BS00-3LA3): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA EEC (PRP/HSR) (6GK5204-0BS00-3PA3): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 24V) (6GK5302-7GD00-2EA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations

SCALANCE X302-7 EEC (2x 24V, coated) (6GK5302-7GD00-2GA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 230V) (6GK5302-7GD00-4EA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (2x 230V, coated) (6GK5302-7GD00-4GA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (24V) (6GK5302-7GD00-1EA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (24V, coated) (6GK5302-7GD00-1GA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (230V) (6GK5302-7GD00-3EA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X302-7 EEC (230V, coated) (6GK5302-7GD00-3GA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X304-2FE (6GK5304-2BD00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X306-1LD FE (6GK5306-1BF00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 24V) (6GK5307-2FD00-2EA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations

SCALANCE X307-2 EEC (2x 24V, coated) (6GK5307-2FD00-2GA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 230V) (6GK5307-2FD00-4EA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (2x 230V, coated) (6GK5307-2FD00-4GA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (24V) (6GK5307-2FD00-1EA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (24V, coated) (6GK5307-2FD00-1GA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (230V) (6GK5307-2FD00-3EA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-2 EEC (230V, coated) (6GK5307-2FD00-3GA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-3 (6GK5307-3BL00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-3 (6GK5307-3BL10-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X307-3LD (6GK5307-3BM00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations

SCALANCE X307-3LD (6GK5307-3BM10-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2 (6GK5308-2FL00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2 (6GK5308-2FL10-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LD (6GK5308-2FM00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LD (6GK5308-2FM10-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH (6GK5308-2FN00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH (6GK5308-2FN10-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH+ (6GK5308-2FP00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2LH+ (6GK5308-2FP10-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M (6GK5308-2GG00-2AA2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations

SCALANCE X308-2M (6GK5308-2GG10-2AA2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M PoE (6GK5308-2QG00-2AA2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M PoE (6GK5308-2QG10-2AA2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M TS (6GK5308-2GG00-2CA2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X308-2M TS (6GK5308-2GG10-2CA2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310 (6GK5310-0FA00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310 (6GK5310-0FA10-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310FE (6GK5310-0BA00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X310FE (6GK5310-0BA10-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X320-1 FE (6GK5320-1BD00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations

SCALANCE X320-1-2LD FE (6GK5320-3BF00-2AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE X408-2 (6GK5408-2FD00-2AA2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG00-2ER2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on front) (6GK5324-4GG10-2ER2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG00-2JR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 24V, ports on rear) (6GK5324-4GG10-2JR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-4ER2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-4ER2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-4JR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (2x 100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-4JR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG00-1ER2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on front) (6GK5324-4GG10-1ER2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG00-1JR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (24V, ports on rear) (6GK5324-4GG10-1JR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG00-3ER2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on front) (6GK5324-4GG10-3ER2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG00-3JR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M EEC (100-240VAC/60-250VDC, ports on rear) (6GK5324-4GG10-3JR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (24V, ports on front) (6GK5324-4QG00-1AR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (24V, ports on rear) (6GK5324-4QG00-1HR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-4M PoE (230V, ports on front) (6GK5324-4QG00-3AR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE (230V, ports on rear) (6GK5324-4QG00-3HR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-4M PoE TS (24V, ports on front) (6GK5324-4QG00-1CR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG00-1AR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on front) (6GK5324-0GG10-1AR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG00-1HR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (24V, ports on rear) (6GK5324-0GG10-1HR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG00-3AR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on front) (6GK5324-0GG10-3AR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG00-3HR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations

SCALANCE XR324-12M (230V, ports on rear) (6GK5324-0GG10-3HR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS (24V) (6GK5324-0GG00-1CR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SCALANCE XR324-12M TS (24V) (6GK5324-0GG10-1CR2): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET SCALANCE X308-2 (6AG1308-2FL10-4AA3): All versions < V4.1.3	Update to V4.1.3 https://support.industry.siemens.com/cs/document/109773547/ See further 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:

- Configure ACLs to only allow Web-based management from trusted IP Adresses
- Disable web-based management (WBM) and use SSH to configure the device

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-2019-13933

Affected devices contain a vulnerability that allows an unauthenticated attacker to violate access-control rules. The vulnerability can be triggered by sending GET request to specific uniform resource locator on the web configuration interface of the device.

The security vulnerability could be exploited by an attacker with network access to the affected systems. An attacker could use the vulnerability to obtain sensitive information or change the device configuration.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score   8.8
CVSS Vector   CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:L/E:P/RL:O/RC:C
CWE   CWE-306: Missing Authentication for Critical Function

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

• Maxim Rupp for coordinated disclosure

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 (2020-01-14):   Publication Date
V1.1 (2022-02-08):   Specifically added that SCALANCE X204RNA devices do not have any fix planned
V1.2 (2022-06-14):   Fix planned for SCALANCE X204RNA devices. Expanded SCALANCE X-300 switch family list
V1.3 (2022-12-13):   Added fix for SCALANCE X-200RNA devices

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.