SSA-602936: Multiple Vulnerabilities in SCALANCE SC-600 Family before V3.1

Publication Date:	2024-02-13
Last Update:	2024-02-13
Current Version:	V1.0
CVSS v3.1 Base Score:	9.1

SUMMARY

SCALANCE SC-600 Family before V3.1 is affected by multiple vulnerabilities.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens recommends countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions < V3.0.2 affected by CVE-2023-44317, CVE-2023-44373, CVE-2023-49691, CVE-2023-49692	Update to V3.0.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109821991/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions < V3.1 affected by CVE-2023-44319, CVE-2023-44320, CVE-2023-44322	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109827038/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions affected by CVE-2023-44321	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE SC626-2C (6GK5626-2GS00-2AC2): All versions < V3.0.2 affected by CVE-2023-44317, CVE-2023-44373, CVE-2023-49691, CVE-2023-49692	Update to V3.0.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109821991/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC626-2C (6GK5626-2GS00-2AC2): All versions < V3.1 affected by CVE-2023-44319, CVE-2023-44320, CVE-2023-44322	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109827038/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC626-2C (6GK5626-2GS00-2AC2): All versions affected by CVE-2023-44321	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions < V3.0.2 affected by CVE-2023-44317, CVE-2023-44373, CVE-2023-49691, CVE-2023-49692	Update to V3.0.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109821991/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions < V3.1 affected by CVE-2023-44319, CVE-2023-44320, CVE-2023-44322	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109827038/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions affected by CVE-2023-44321	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions < V3.0.2 affected by CVE-2023-44317, CVE-2023-44373, CVE-2023-49691, CVE-2023-49692	Update to V3.0.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109821991/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions < V3.1 affected by CVE-2023-44319, CVE-2023-44320, CVE-2023-44322	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109827038/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions affected by CVE-2023-44321	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions < V3.0.2 affected by CVE-2023-44317, CVE-2023-44373, CVE-2023-49691, CVE-2023-49692	Update to V3.0.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109821991/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions < V3.1 affected by CVE-2023-44319, CVE-2023-44320, CVE-2023-44322	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109827038/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions affected by CVE-2023-44321	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions < V3.0.2 affected by CVE-2023-44317, CVE-2023-44373, CVE-2023-49691, CVE-2023-49692	Update to V3.0.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109821991/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions < V3.1 affected by CVE-2023-44319, CVE-2023-44320, CVE-2023-44322	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109827038/ See further recommendations from section Workarounds and Mitigations
SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions affected by CVE-2023-44321	Currently no fix is planned See 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:

- Restrict access to application webserver for trusted users only

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 SC-600 devices are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

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-2023-44317

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-2023-44319

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-2023-49691

An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the handling of the DDNS configuration. This could allow malicious local administrators to issue commands on system level after a successful IP address update.

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-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vulnerability CVE-2023-49692

An Improper Neutralization of Special Elements used in an OS Command with root privileges vulnerability exists in the parsing of the IPSEC configuration. This could allow malicious local administrators to issue commands on system level after a new connection is established.

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-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

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 (2024-02-13):	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.