SSA-690517: Multiple Vulnerabilities in SCALANCE W700 802.11 AX Family

Publication Date:	2024-06-11
Last Update:	2024-06-11
Current Version:	V1.0
CVSS v3.1 Base Score:	9.1

SUMMARY

SCALANCE W700 802.11 AX Family is affected by multiple vulnerabilities.

Siemens recommends countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE WAM763-1 (6GK5763-1AL00-7DA0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WAM763-1 (ME) (6GK5763-1AL00-7DC0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WAM763-1 (US) (6GK5763-1AL00-7DB0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WAM766-1 (EU) (6GK5766-1GE00-7DA0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WAM766-1 (ME) (6GK5766-1GE00-7DC0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WAM766-1 EEC (EU) (6GK5766-1GE00-7TA0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WAM766-1 EEC (ME) (6GK5766-1GE00-7TC0): All versions affected by all CVEs	Currently no fix is planned

SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WUM763-1 (6GK5763-1AL00-3AA0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WUM763-1 (6GK5763-1AL00-3DA0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WUM763-1 (US) (6GK5763-1AL00-3AB0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WUM763-1 (US) (6GK5763-1AL00-3DB0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WUM766-1 (EU) (6GK5766-1GE00-3DA0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WUM766-1 (ME) (6GK5766-1GE00-3DC0): All versions affected by all CVEs	Currently no fix is planned
SCALANCE WUM766-1 (US) (6GK5766-1GE00-3DB0): All versions affected by all CVEs	Currently no fix is planned

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 W-700 products are wireless communication devices based on IEEE 802.11ax or 802.11n 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.

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-2022-46144

Affected devices do not properly process CLI commands after a user forcefully quitted the SSH connection. This could allow an authenticated attacker to make the CLI via SSH or serial interface irresponsive.

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:N/A:H/E:P/RL:O/RC:C
CWE	CWE-664: Improper Control of a Resource Through its Lifetime

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-2023-44373

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

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')

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 (2024-06-11):	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.