SSA-565386: Third-Party Component Vulnerabilities in SCALANCE W-700 IEEE 802.11ax devices before V2.0

Publication Date: 2023-03-14
Last Update: 2023-03-14
Current Version: V1.0
CVSS v3.1 Base Score: 8.1

SUMMARY

Multiple vulnerabilities affecting various third-party components of SCALANCE W-700 IEEE 802.11ax devices before V2.0 could allow an attacker to cause a denial of service condition, disclose sensitive data or violate the system integrity.

Siemens has released an update for SCALANCE W-700 IEEE 802.11ax and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE WAM763-1 (6GK5763-1AL00-7DA0): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WAM766-1 (EU) (6GK5766-1GE00-7DA0): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WAM766-1 EEC (EU) (6GK5766-1GE00-7TA0): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WUM763-1 (6GK5763-1AL00-3AA0): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WUM763-1 (6GK5763-1AL00-3DA0): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/
SCALANCE WUM766-1 (EU) (6GK5766-1GE00-3DA0): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/

SCALANCE WUM766-1 (US) (6GK5766-1GE00-3DB0): All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109815650/

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 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 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-2018-12886

stack_protect_prologue in cfgexpand.c and stack_protect_epilogue in function.c in GNU Compiler Collection (GCC) 4.1 through 8 (under certain circumstances) generate instruction sequences when targeting ARM targets that spill the address of the stack protector guard, which allows an attacker to bypass the protection of -fstack-protector, -fstack-protector-all, -fstack-protector-strong, and -fstack-protector-explicit against stack overflow by controlling what the stack canary is compared against.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-209: Generation of Error Message Containing Sensitive Information

Vulnerability CVE-2018-25032

zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2021-42373

A NULL pointer dereference in Busybox's man applet leads to denial of service when a section name is supplied but no page argument is given.

CVSS v3.1 Base Score	5.1
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2021-42374

An out-of-bounds heap read in Busybox's unlzma applet leads to information leak and denial of service when crafted LZMA-compressed input is decompressed. This can be triggered by any applet/format that internally supports LZMA compression.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-42375

An incorrect handling of a special element in Busybox's ash applet leads to denial of service when processing a crafted shell command, due to the shell mistaking specific characters for reserved characters. This may be used for DoS under rare conditions of filtered command input.

CVSS v3.1 Base Score	4.1
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-42376

A NULL pointer dereference in Busybox's hush applet leads to denial of service when processing a crafted shell command, due to missing validation after a \x03 delimiter character. This may be used for DoS under very rare conditions of filtered command input.

CVSS v3.1 Base Score	4.1
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2021-42377

An attacker-controlled pointer free in Busybox's hush applet leads to denial of service and possible code execution when processing a crafted shell command, due to the shell mishandling the &&& string. This may be used for remote code execution under rare conditions of filtered command input.

CVSS v3.1 Base Score	6.4
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-763: Release of Invalid Pointer or Reference

Vulnerability CVE-2021-42378

A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the getvar_i function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42379

A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the next_input_file function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42380

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the clrvar function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42381

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the hash_init function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42382

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the getvar_s function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42383

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the evaluate function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42384

A use-after-free in Busybox's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the handle_special function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42385

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the evaluate function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42386

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the nvalloc function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-23395

jQuery Cookie 1.4.1 is affected by prototype pollution, which can lead to DOM cross-site scripting (XSS).

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

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 (2023-03-14): 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.