SSA-457702: Wi-Fi Encryption Bypass Vulnerabilities in SCALANCE W700 Product Family

Publication Date: 2023-11-14
Last Update: 2024-04-09
Current Version: V1.1
CVSS v3.1 Base Score: 8.4

SUMMARY

The SCALANCE W700 devices are affected by Wi-Fi encryption bypass vulnerabilities ("Framing Frames") that could allow an attacker to disclose sensitive information, to steal the victims session or to execute denial-of-service attacks.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W721-1 RJ45 (6GK5721-1FC00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W722-1 RJ45 (6GK5722-1FC00-0AC0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AA6): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W734-1 RJ45 (6GK5734-1FX00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W734-1 RJ45 (USA) (6GK5734-1FX00-0AB6): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W738-1 M12 (6GK5738-1GY00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W738-1 M12 (6GK5738-1GY00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 M12 (6GK5748-1GD00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 M12 (6GK5748-1GD00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W748-1 RJ45 (6GK5748-1FC00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W761-1 RJ45 (6GK5761-1FC00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 M12 EEC (6GK5774-1FY00-0TB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AA6): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (6GK5774-1FX00-0AC0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W774-1 RJ45 (USA) (6GK5774-1FX00-0AB6): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 (6GK5778-1GY00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 (6GK5778-1GY00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 EEC (6GK5778-1GY00-0TA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W778-1 M12 EEC (USA) (6GK5778-1GY00-0TB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-1 RJ45 (6GK5786-1FC00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 RJ45 (6GK5786-2FC00-0AC0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 SFP (6GK5786-2FE00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2 SFP (6GK5786-2FE00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W786-2IA RJ45 (6GK5786-2HC00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 M12 (6GK5788-1GD00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 M12 (6GK5788-1GD00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-1 RJ45 (6GK5788-1FC00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 (6GK5788-2GD00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 (6GK5788-2GD00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 M12 EEC (6GK5788-2GD00-0TC0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AA0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AB0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W788-2 RJ45 (6GK5788-2FC00-0AC0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1748-1 M12 (6GK5748-1GY01-0AA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1748-1 M12 (6GK5748-1GY01-0TA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SCALANCE WAM763-1 (6GK5763-1AL00-7DA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 (EU) (6GK5766-1GE00-7DA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 (US) (6GK5766-1GE00-7DB0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 EEC (EU) (6GK5766-1GE00-7TA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE WAM766-1 EEC (US) (6GK5766-1GE00-7TB0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE WUM763-1 (6GK5763-1AL00-3AA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE WUM763-1 (6GK5763-1AL00-3DA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 (EU) (6GK5766-1GE00-3DA0): All versions affected by CVE-2024-30190, CVE-2024-30191	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE WUM766-1 (US) (6GK5766-1GE00-3DB0): All versions affected by CVE-2024-30190, CVE-2024-30191	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:

- CVE-2024-30189, CVE-2024-30191:
  - Use TLS based communication
  - Use VLAN based segregation of clients (802.1q)
- CVE-2024-30191:
  - Recommendation for upper layers: Do not allow associations to use MAC addresses that are duplicates used by internal services on the LAN
  - Use Wi-Fi Management Frame Protection (802.11w)

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-1700 products are wireless communication devices based on IEEE 802.11ac 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.

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-2024-30189

This CVE refers to Scenario 1 "Leak frames from the Wi-Fi queue" of CVE-2022-47522.

Affected devices queue frames in order to subsequently change the security context and leak the queued frames. This could allow a physically proximate attacker to intercept (possibly cleartext) target-destined frames.

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N
CWE	CWE-290: Authentication Bypass by Spoofing

Vulnerability CVE-2024-30190

This CVE refers to Scenario 2 "Abuse the queue for network disruptions" of CVE-2022-47522.

Affected devices can be tricked into enabling its power-saving mechanisms for a victim client. This could allow a physically proximate attacker to execute disconnection and denial-of-service attacks.

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:C/C:N/I:N/A:H
CWE	CWE-290: Authentication Bypass by Spoofing

Vulnerability CVE-2024-30191

This CVE refers to Scenario 3 "Override client's security context" of CVE-2022-47522.

Affected devices can be tricked into associating a newly negotiated, attacker-controlled, security context with frames belonging to a victim. This could allow a physically proximate attacker to decrypt frames meant for the victim.

CVSS v3.1 Base Score	8.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H
CWE	CWE-290: Authentication Bypass by Spoofing

ADDITIONAL INFORMATION

For more information regarding the listed vulnerabilities see the original published paper (https://papers.mathyvanhoef.com/usenix2023-wifi.pdf).

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 (2023-11-14):	Publication Date
V1.1 (2024-04-09):	Split CVE-2022-47522 in three separate CVE's: CVE-2024-30189 for Scenario 1, CVE-2024-30190 for Scenario 2, CVE-2024-30191 for Scenario 3

TERMS OF USE