Siemens Security Advisory by Siemens ProductCERT

SSA-019200: Multiple Vulnerabilities in SCALANCE W-700 IEEE 802.11n Devices Before V6.6.0

Publication Date:	2026-04-14
Last Update:	2026-04-14
Current Version:	V1.0
CVSS v3.1 Base Score:	9.1
CVSS v4.0 Base Score:	9.4

▼ SUMMARY

SCALANCE W-700 IEEE 802.11n family before V6.6.0 are affected by multiple vulnerabilities.

Siemens has released a new version for SCALANCE W-700 IEEE 802.11n family and recommends to update to the latest version.

▼ KNOWN AFFECTED PRODUCTS

Un-/Collapse All

Affected Product and Versions	Remediation
SCALANCE W-700 IEEE 802.11n family	Show more details

▼ MITIGATIONS

Siemens has identified the following specific mitigations that customers can apply to reduce the risk:

- CVE-2020-24588
  - As these vulnerabilities can only be exploited within Wi-Fi range, when possible reduce Wi-Fi transmission power or make sure to have the devices in private areas with physical access controls
  - Disable A-MSDU, if possible
- CVE-2020-26139
  - As these vulnerabilities can only be exploited within Wi-Fi range, when possible reduce Wi-Fi transmission power or make sure to have the devices in private areas with physical access controls
- CVE-2020-26140
  - As these vulnerabilities can only be exploited within Wi-Fi range, when possible reduce Wi-Fi transmission power or make sure to have the devices in private areas with physical access controls
- CVE-2020-26141
  - As these vulnerabilities can only be exploited within Wi-Fi range, when possible reduce Wi-Fi transmission power or make sure to have the devices in private areas with physical access controls
- CVE-2020-26143
  - As these vulnerabilities can only be exploited within Wi-Fi range, when possible reduce Wi-Fi transmission power or make sure to have the devices in private areas with physical access controls

- CVE-2020-26144
  - As these vulnerabilities can only be exploited within Wi-Fi range, when possible reduce Wi-Fi transmission power or make sure to have the devices in private areas with physical access controls
- CVE-2020-26146
  - As these vulnerabilities can only be exploited within Wi-Fi range, when possible reduce Wi-Fi transmission power or make sure to have the devices in private areas with physical access controls
- CVE-2020-26147
  - As these vulnerabilities can only be exploited within Wi-Fi range, when possible reduce Wi-Fi transmission power or make sure to have the devices in private areas with physical access controls

Product-specific remediations or mitigations can be found in the section Known Affected Products.
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

▼ VULNERABILITY DESCRIPTION

Un-/Collapse All

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-2020-24588

▶ Vulnerability CVE-2020-26139

▶ Vulnerability CVE-2020-26140

▶ Vulnerability CVE-2020-26141

▶ Vulnerability CVE-2020-26143

▶ Vulnerability CVE-2020-26144

▶ Vulnerability CVE-2020-26146

▶ Vulnerability CVE-2020-26147

▶ Vulnerability CVE-2021-3712

▶ Vulnerability CVE-2022-0778

▶ Vulnerability CVE-2022-31765

▶ Vulnerability CVE-2022-36323

▶ Vulnerability CVE-2022-36324

▶ **Vulnerability CVE-2022-36325**

▶ **Vulnerability CVE-2023-44373**

▼ 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 (2026-04-14):		Publication Date

▼ TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.