SSA-392912: Multiple Denial Of Service Vulnerabilities in SCALANCE W1700 Devices

Publication Date: 2022-04-12
Last Update: 2022-04-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.4

SUMMARY

Vulnerabilities have been identified in devices of the SCALANCE W-1700 (11ac) family that could allow an attacker to cause various denial of service conditions.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further 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:

- For **CVE-2022-28329**: Deactivate the RemoteCapture feature if not required. This feature is deactivated by default
- For **CVE-2022-28329**: Restrict network access to the RemoteCapture feature to trusted communication partners

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-1700 products are wireless communication devices based on IEEE 802.11 standards. 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-2022-27481

Affected devices do not properly handle resources of ARP requests. This could allow an attacker to cause a race condition that leads to a crash of the entire device.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2022-28328

Affected devices do not properly handle malformed Multicast LLC frames. This could allow an attacker to trigger a denial of service condition.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2022-28329

Affected devices do not properly handle malformed TCP packets received over the RemoteCapture feature. This could allow an attacker to lead to a denial of service condition which only affects the port used by the RemoteCapture feature.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

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 (2022-04-12): 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.