SSA-363821: Multiple Vulnerabilities in SCALANCE X-200RNA Switch Devices before V3.2.7

Publication Date: 2022-12-13
Last Update: 2022-12-13
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

SUMMARY

SCALANCE X-200RNA switch devices before V3.2.7 contain multiple vulnerabilities that could allow an attacker to cause a denial of service condition, to extract sensitive information or to hijack existing sessions.

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 X204RNA (HSR) (6GK5204-0BA00-2MB2): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA (PRP) (6GK5204-0BA00-2KB2): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA EEC (HSR) (6GK5204-0BS00-2NA3): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA EEC (PRP) (6GK5204-0BS00-3LA3): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ See further recommendations from section Workarounds and Mitigations
SCALANCE X204RNA EEC (PRP/HSR) (6GK5204-0BS00-3PA3): All versions < V3.2.7	Update to V3.2.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109814809/ 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:

- Restrict access to the affected systems, especially to ports 22/tcp, 80/tcp, 443/tcp and 161/udp to trusted IP addresses only
- Disable the SNMP service if not required, and if disabling is supported by the product

- Deactivate the web server if not required, and if deactivation is supported by the product

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

The SCALANCE X-204RNA Industrial Ethernet network access points enable the cost-effective connection of non-PRP terminal devices to separate parallel networks, where a high availability is required.

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-2022-46350

The integrated web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. This can be used by an attacker to trigger a malicious request on the affected device.

CVSS v3.1 Base Score	7.9
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

Vulnerability CVE-2022-46351

Specially crafted PROFINET DCP packets could cause a denial of service condition of affected products on a local Ethernet segment (Layer 2).

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2022-46352

Specially crafted PROFINET DCP packets could cause a denial of service condition of affected products.

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-400: Uncontrolled Resource Consumption

Vulnerability CVE-2022-46353

The webserver of affected devices calculates session ids and nonces in an insecure manner. This could allow an unauthenticated remote attacker to brute-force session ids and hijack existing sessions.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-330: Use of Insufficiently Random Values

Vulnerability CVE-2022-46354

The webserver of an affected device is missing specific security headers. This could allow an remote attacker to extract confidential session information under certain circumstances.

CVSS v3.1 Base Score	2.6
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2022-46355

The affected products are vulnerable to an “Exposure of Sensitive Information to an Unauthorized Actor” vulnerability by leaking sensitive data in the HTTP Referer.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

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 (2022-12-13): 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.