SSA-792319: Missing Read Out Protection in SENTRON 7KM PAC3x20 Devices

Publication Date: 2024-03-12
Last Update: 2024-03-12
Current Version: V1.0
CVSS v3.1 Base Score: 4.6
CVSS v4.0 Base Score: 5.1

SUMMARY

The read out protection of the internal flash of affected devices was not properly set at the end of the manufacturing process.

An attacker with physical access to the device could read out the data.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SENTRON 7KM PAC3120 AC/DC (7KM3120-0BA01-1DA0): All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...) affected by all CVEs	Update to V3.3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109780936/ See further recommendations from section Workarounds and Mitigations
SENTRON 7KM PAC3120 DC (7KM3120-1BA01-1EA0): All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...) affected by all CVEs	Update to V3.3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109780936/ See further recommendations from section Workarounds and Mitigations
SENTRON 7KM PAC3220 AC/DC (7KM3220-0BA01-1DA0): All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...) affected by all CVEs	Update to V3.3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109780938/ See further recommendations from section Workarounds and Mitigations
SENTRON 7KM PAC3220 DC (7KM3220-1BA01-1EA0): All versions >= V3.2.3 < V3.3.0 only when manufactured between LQN231003... and LQN231215... (with LQNYYMMDD...) affected by all CVEs	Update to V3.3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109780938/ 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 physical access to the device to trusted personnel

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

SENTRON PAC Meter products are power measuring devices for precise energy management and transparent information acquisition.

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-2024-21483

The read out protection of the internal flash of affected devices was not properly set at the end of the manufacturing process.

An attacker with physical access to the device could read out the data.

CVSS v3.1 Base Score	4.6
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v4.0 Base Score	5.1
CVSS Vector	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-284: Improper Access Control

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 (2024-03-12): 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.