SSA-325383: Multiple Vulnerabilities in SCALANCE LPE9403 before V2.1

Publication Date: 2023-05-09
Last Update: 2023-05-09
Current Version: V1.0
CVSS v3.1 Base Score: 9.9

SUMMARY

SCALANCE LPE9403 is affected by multiple vulnerabilities that could allow an attacker to impact its confidentiality, integrity and availability.

Siemens has released an update for the SCALANCE LPE9403 and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE LPE9403 (6GK5998-3GS00-2AC2): All versions < V2.1	Update to V2.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109817856/

WORKAROUNDS AND MITIGATIONS

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 LPE9000 (Local Processing Engine) extends the SCALANCE family portfolio by a component that provides computing power for a wide range of applications in the network, close to the process – Edge Computing.

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-2023-27407

The web based management of affected device does not properly validate user input, making it susceptible to command injection. This could allow an authenticated remote attacker to access the underlying operating system as the root user.

CVSS v3.1 Base Score	9.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2023-27408

The `i2c` mutex file is created with the permissions bits of `-rw-rw-rw-`. This file is used as a mutex for multiple applications interacting with i2c. This could allow an authenticated attacker with access to the SSH interface on the affected device to interfere with the integrity of the mutex and the data it protects.

CVSS v3.1 Base Score	3.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-378: Creation of Temporary File With Insecure Permissions

Vulnerability CVE-2023-27409

A path traversal vulnerability was found in the `deviceinfo` binary via the `mac` parameter. This could allow an authenticated attacker with access to the SSH interface on the affected device to read the contents of any file named `address`.

CVSS v3.1 Base Score	2.5
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2023-27410

A heap-based buffer overflow vulnerability was found in the `edgebox_web_app` binary. The binary will crash if supplied with a backup password longer than 255 characters. This could allow an authenticated privileged attacker to cause a denial of service.

CVSS v3.1 Base Score	2.7
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

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 (2023-05-09):	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.