SSA-222547: Third-Party Component Vulnerabilities in SCALANCE LPE9403 before V2.0

Publication Date:	2022-06-14
Last Update:	2022-06-14
Current Version:	V1.0
CVSS v3.1 Base Score:	9.8

SUMMARY

Multiple vulnerabilities in the third-party components CivetWeb, Docker, Linux Kernel and systemd could allow an attacker to impact SCALANCE LPE9403 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 < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109811123/

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-2020-27304

The CivetWeb web library does not validate uploaded filepaths when running on an OS other than Windows, when using the built-in HTTP form-based file upload mechanism, via the mg_handle_form_request API. Web applications that use the file upload form handler, and use parts of the user-controlled filename in the output path, are susceptible to directory traversal

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2021-20317

A corrupted timer tree caused the task wakeup to be missing in the timerqueue_add function in lib/timerqueue.c. This flaw allows a local attacker with special user privileges to cause a denial of service, slowing and eventually stopping the system while running OSP.

CVSS v3.1 Base Score	4.4
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-665: Improper Initialization

Vulnerability CVE-2021-33910

The use of alloca function with an uncontrolled size in function unit_name_path_escape allows a local attacker, able to mount a filesystem on a very long path, to crash systemd and the whole system by allocating a very large space in the stack.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2021-36221

A race condition vulnerability was found in Go. The incoming requests body weren't closed after the handler panic and as a consequence this could lead to ReverseProxy crash.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/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-2021-39293

The fix for CVE-2021-33196 can be bypassed by crafted inputs. As a result, the NewReader and OpenReader functions in archive/zip can still cause a panic or an unrecoverable fatal error when reading an archive that claims to contain a large number of files, regardless of its actual size.

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-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2021-41089

A vulnerability was found in Moby (Docker Engine) where attempting to copy files using `docker cp` into a specially-crafted container can result in Unix file permission changes for existing files in the host's filesystem, widening access to others. This bug does not directly allow files to be read, modified, or executed without an additional cooperating process.

CVSS v3.1 Base Score	2.8
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-281: Improper Preservation of Permissions

Vulnerability CVE-2021-41091

A vulnerability was found in Moby (Docker Engine) where the data directory (typically `/var/lib/docker`) contained subdirectories with insufficiently restricted permissions, allowing otherwise unprivileged Linux users to traverse directory contents and execute programs. When containers included executable programs with extended permission bits (such as `setuid`), unprivileged Linux users could discover and execute those programs. When the UID of an unprivileged Linux user on the host collided with the file owner or group inside a container, the unprivileged Linux user on the host could discover, read, and modify those files.

CVSS v3.1 Base Score	6.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2021-41092

A vulnerability was found in the Docker CLI where running `docker login my-private-registry.example.com` with a misconfigured configuration file (typically `~/.docker/config.json`) listing a `credsStore` or `credHelpers` that could not be executed would result in any provided credentials being sent to `registry-1.docker.io` rather than the intended private registry.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2021-41103

A vulnerability was found in containerd where container root directories and some plugins had insufficiently restricted permissions, allowing otherwise unprivileged Linux users to traverse directory contents and execute programs. When containers included executable programs with extended permission bits (such as setuid), unprivileged Linux users could discover and execute those programs. When the UID of an unprivileged Linux user on the host collided with the file owner or group inside a container, the unprivileged Linux user on the host could discover, read, and modify those files.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2022-0847

A vulnerability was found in the way the “flags” member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this to write to pages in the page cache backed by read only files and as such escalate their privileges on the system.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-281: Improper Preservation of Permissions

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 (2022-06-14):	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.