SSA-330556: PwnKit Vulnerability in SCALANCE LPE9403 and SINUMERIK Edge Products (CVE-2021-4034)

Publication Date: 2022-06-14
Last Update: 2022-06-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

The products listed below contain a local privilege escalation vulnerability (CVE-2021-4034) found on polkit's pkexec utility, that could allow an unprivileged user to gain administrative rights.

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 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/ See further recommendations from section Workarounds and Mitigations
SINUMERIK Edge: All versions < V3.3.0	Update to V3.3.0 or later version Use the internal update mechanism of the device(s). See Documentation for further information. 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 system access to authorized personnel and follow a least privilege approach
- Temporary mitigation exists at the expense of pkexec's capabilities. By removing SUID permissions, the program cannot run processes as root. However, any processes that rely on it for normal operation will be affected

  - SUID permission can be removed with chmod, as follows: chmod 0755 /usr/bin/pkexec

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

A combination of hardware and software, Siemens' SINUMERIK Edge provides a machine-oriented platform for apps that facilitate digital production support and optimization.

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-2021-4034

A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

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:U/RC:C
CWE	CWE-787: Out-of-bounds Write

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.