SSA-634640: Weak Authentication Vulnerability in Siemens Industrial Edge Devices

Publication Date: 2025-04-08
Last Update: 2025-07-08
Current Version: V1.1
CVSS v3.1 Base Score: 9.8
CVSS v4.0 Base Score: 9.3

SUMMARY

Siemens Industrial Edge Devices contain a weak authentication vulnerability that could facilitate an unauthenticated remote attacker to circumvent authentication and impersonate a legitimate user.

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
Industrial Edge Devices:	See below See recommendations from section Workarounds and Mitigations
Industrial Edge Own Device (IEOD): All versions < V1.21.1-1-a affected by CVE-2024-54092	Update to V1.21.1-1-a or later version https://docs.industrial-operations-x.siemens.cloud/r/en-us/v25.02/industrial-edge-platform-operation-what-s-new/device-release-notes/release-notes-industrial-edge-own-device See further recommendations from section Workarounds and Mitigations
Industrial Edge Virtual Device: All versions < V1.21.1-1-a affected by CVE-2024-54092	Update to V1.21.1-1-a or later version https://docs.industrial-operations-x.siemens.cloud/r/en-us/v25.02/industrial-edge-platform-operation-what-s-new/device-release-notes/release-notes-industrial-edge-virtual-device See further recommendations from section Workarounds and Mitigations
SCALANCE LPE9413 (6GK5998-3GS01-2AC2): All versions < V2.1 affected by CVE-2024-54092	Update to V2.1 or later version https://docs.eu1.edge.siemens.cloud/release_notes/device_release_notes/LPE9413.html See further recommendations from section Workarounds and Mitigations
SIMATIC IPC BX-39A Industrial Edge Device: All versions < V3.0 affected by CVE-2024-54092	Update to V3.0 or later version https://docs.industrial-operations-x.siemens.cloud/r/en-us/v3.0/simatic-ipc-ied-os/release-notes See further recommendations from section Workarounds and Mitigations

SIMATIC IPC BX-59A Industrial Edge Device: All versions < V3.0 affected by CVE-2024-54092	Update to V3.0 or later version https://docs.industrial-operations-x.siemens.cloud/r/en-us/v3.0/simatic-ipc-ied-os/release-notes See further recommendations from section Workarounds and Mitigations
SIMATIC IPC127E Industrial Edge Device: All versions < V3.0 affected by CVE-2024-54092	Update to V3.0 or later version https://docs.industrial-operations-x.siemens.cloud/r/en-us/v3.0/simatic-ipc-ied-os/release-notes See further recommendations from section Workarounds and Mitigations
SIMATIC IPC227E Industrial Edge Device: All versions < V3.0 affected by CVE-2024-54092	Update to V3.0 or later version https://docs.industrial-operations-x.siemens.cloud/r/en-us/v3.0/simatic-ipc-ied-os/release-notes See further recommendations from section Workarounds and Mitigations
SIMATIC IPC427E Industrial Edge Device: All versions < V3.0 affected by CVE-2024-54092	Update to V3.0 or later version https://docs.industrial-operations-x.siemens.cloud/r/en-us/v3.0/simatic-ipc-ied-os/release-notes See further recommendations from section Workarounds and Mitigations
SIMATIC IPC847E Industrial Edge Device: All versions < V3.0 affected by CVE-2024-54092	Update to V3.0 or later version https://docs.industrial-operations-x.siemens.cloud/r/en-us/v3.0/simatic-ipc-ied-os/release-notes 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:

- CVE-2024-54092: Ensure network access to affected products is limited to trusted parties only

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

Industrial Edge Own Device (IEOD) offers the Industrial Edge functionality and user experience on top of hardware by customer-choice.

Industrial Edge Virtual Device (IEVD) offers you the Industrial Edge Device functionality without the need of dedicated physical hardware devices.

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.

SIMATIC IPC Industrial Edge devices are industrial PCs that are pre-configured with the Industrial Edge Device software.

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-2024-54092

Affected devices do not properly enforce user authentication on specific API endpoints when identity federation is used. This could facilitate an unauthenticated remote attacker to circumvent authentication and impersonate a legitimate user. Successful exploitation requires that identity federation is currently or has previously been used and the attacker has learned the identity of a legitimate user.

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
CVSS v4.0 Base Score	9.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-1390: Weak Authentication

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 (2025-04-08): Publication Date
V1.1 (2025-07-08): Added fix for SCALANCE LPE9413 (6GK5998-3GS01-2AC2)

TERMS OF USE