Siemens Security Advisory by Siemens ProductCERT

SSA-014678: Authorization Bypass Vulnerability in Industrial Edge Device Kit

Publication Date:	2026-01-13
Last Update:	2026-01-13
Current Version:	V1.0
CVSS v3.1 Base Score:	10.0
CVSS v4.0 Base Score:	10.0

▼ SUMMARY

Users of Industrial Edge Devices are advised to consult the respective Security Advisories for their devices (for Siemens Industrial Edge devices see Additional Information).

Industrial Edge Device Kit contains an authorization bypass vulnerability that could facilitate an unauthenticated remote attacker to circumvent authentication and impersonate a legitimate user.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where fixes are not, or not yet available.

▼ KNOWN AFFECTED PRODUCTS

Un-/Collapse All

Affected Product and Versions	Remediation
Industrial Edge Device Kit - arm64 V1.5 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.6 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.7 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.8 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.9 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.10 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.11 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations

Industrial Edge Device Kit - arm64 V1.12 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.13 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.14 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.15 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.16 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.17 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.18 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.19 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.20 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.21 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.22 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.23 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.24 All versions < V1.24.2 affected by CVE-2025-40805	Update to V1.24.2 or later version See further recommendations from section Mitigations
Industrial Edge Device Kit - arm64 V1.25 All versions < V1.25.1 affected by CVE-2025-40805	Update to V1.25.1 or later version See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.5 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.6 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations

Industrial Edge Device Kit - x86-64 V1.7 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.8 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.9 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.10 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.11 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.12 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.13 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.14 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.15 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.16 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.17 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.18 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.19 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.20 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.21 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.22 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations

Industrial Edge Device Kit - x86-64 V1.23 All versions affected by CVE-2025-40805	Currently no fix is planned See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.24 All versions < V1.24.2 affected by CVE-2025-40805	Update to V1.24.2 or later version See further recommendations from section Mitigations
Industrial Edge Device Kit - x86-64 V1.25 All versions < V1.25.1 affected by CVE-2025-40805	Update to V1.25.1 or later version See further recommendations from section Mitigations

▼ MITIGATIONS

Siemens has identified the following specific mitigations that customers can apply to reduce the risk:

- Ensure network access to affected products is limited to trusted parties only

Product-specific remediations or mitigations can be found in the section Known Affected Products.
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

▼ VULNERABILITY DESCRIPTION

Un-/Collapse All

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-2025-40805

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

CVSS v3.1 Base Score	10.0
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v4.0 Base Score	10.0
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
CWE	CWE-639: Authorization Bypass Through User-Controlled Key

▼ ADDITIONAL INFORMATION

Downstream information about Industrial Edge Devices built on an affected device kit:

- For devices built by Siemens: https://cert-portal.siemens.com/productcert/html/ssa-001536.html

Industrial Edge Device Kit version lines that are not maintained anymore can be updated to newer version lines that either have received an update or were released including the fix already.

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 (2026-01-13):		Publication Date

▼ TERMS OF USE

The use of Siemens Security Advisories is subject to the terms and conditions listed on: https://www.siemens.com/productcert/terms-of-use.