Siemens Security Advisory by Siemens ProductCERT

SSA-928984: Heap-based Buffer Overflow Vulnerability in User Management Component (UMC)

Publication Date:	2024-12-16
Last Update:	2026-01-13
Current Version:	V1.4
CVSS v3.1 Base Score:	9.8
CVSS v4.0 Base Score:	9.3

▼ SUMMARY

Siemens User Management Component (UMC) is affected by a heap-based buffer overflow vulnerability which could allow an unauthenticated remote attacker arbitrary code execution.

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
Opcenter Execution Foundation All versions < V2501.0001 affected by CVE-2024-49775	Update to V2501.0001 or later version https://support.sw.siemens.com/product/219646572/ See further recommendations from section Mitigations
Opcenter Intelligence All versions < V2501.0001 affected by CVE-2024-49775	Update to V2501.0001 or later version https://support.sw.siemens.com/product/287414453/ See further recommendations from section Mitigations
Opcenter Quality All versions < V2512 affected by CVE-2024-49775	Update to V2512 or later version https://support.sw.siemens.com/product/249261320 See further recommendations from section Mitigations
Opcenter RDnL All versions < V2410 affected by CVE-2024-49775	Update to V2410 or later version https://support.sw.siemens.com/product/297341591/ See further recommendations from section Mitigations
SIMATIC PCS neo	Show more details
SINEC NMS All versions if operated in conjunction with UMC < V2.15 affected by CVE-2024-49775	Update UMC to V2.15.1.1 or later compatible version https://support.industry.siemens.com/cs/ww/en/view/109987708/

	See further recommendations from section Mitigations
Totally Integrated Automation Portal (TIA Portal)	Show more details

▼ KNOWN NOT AFFECTED PRODUCTS

Un-/Collapse All

Known Not Affected Products	Reason
Desigo ABT All versions not affected by CVE-2024-49775	While TIA Portal is included as part of the ABT Site installation, neither ABT itself nor the incorporated TIA version uses or installs the affected User Management Component (UMC). As a result, any standalone ABT installation remains unaffected by this issue. (Component Not Present)

▼ MITIGATIONS

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

- In addition if no RT server machines are used, port 4004 can be blocked completely
- Filter the ports 4002 and 4004 to only accept connections to/from the IP addresses of machines that run UMC and are part of the UMC network e.g. with an external firewall

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-2024-49775

Affected products contain a heap-based buffer overflow vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to execute arbitrary code.

CVSS v3.1 Base Score	9.8
CVSS v3.1 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 v4.0 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-122: Heap-based Buffer Overflow

▼ ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Tenable for coordinated disclosure

▼ ADDITIONAL INFORMATION

Totally Integrated Automation Portal (TIA Portal) V20 [1] incorporates a fixed UMC version that is not affected by CVE-2024-49775.

[1] https://support.industry.siemens.com/cs/document/109963850

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	(2024-12-16):	Publication Date
V1.1	(2025-03-11):	Added fix for SIMATIC PCS neo V4.1
V1.2	(2025-05-13):	Added remediation for Totally Integrated Automation Portal (TIA Portal) V17, V18 and V19. Updated remediation for SINEC NMS to point directly to the update of UMC
V1.3	(2025-06-10):	Added fix for Opcenter Execution Foundation, Opcenter Intelligence and Opcenter RDnL
V1.4	(2026-01-13):	Added fix for Opcenter Quality

▼ 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.