SSA-722410: Multiple Vulnerabilities in User Management Component (UMC)

Publication Date:	2025-09-09
Last Update:	2025-09-09
Current Version:	V1.0
CVSS v3.1 Base Score:	9.8
CVSS v4.0 Base Score:	9.3

SUMMARY

Siemens' User Management Component (UMC) is affected by multiple vulnerabilities that could allow an unauthenticated remote attacker to execute arbitrary code or to cause a denial of service condition.

Siemens has released a new version for User Management Component (UMC) and recommends to update to the latest version. Siemens recommends specific countermeasures for products where fixes are not, or not yet available.

KNOWN AFFECTED PRODUCTS

Affected Product and Versions	Remediation
SIMATIC PCS neo:	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PCS neo V4.1: All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PCS neo V5.0: All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
User Management Component (UMC): All versions < V2.15.1.3 affected by all CVEs	Update to V2.15.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109991261/ 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:

- In non-networked scenarios/deployments block TCP ports 4002 and 4004 on machines with UMC installed. If the deployment is not using the 'RT Server' type of UMC machine, port 4004 can be blocked everywhere without impacting network functionality for all other UMC machine-types (Server, Ring-Server, Agent).

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

User Management Component (UMC) enables for plant-wide central maintenance of users with optional integration with Microsoft Active Directories.

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-2025-40795

Affected products contain a stack-based buffer overflow vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to execute arbitrary code or to cause a denial of service condition.

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-121: Stack-based Buffer Overflow

Vulnerability CVE-2025-40796

Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2025-40797

Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2025-40798

Affected products contain a out-of-bounds read vulnerability in the integrated UMC component. This could allow an unauthenticated remote attacker to cause a denial of service condition.

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-125: Out-of-bounds Read

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Tenable for coordinated disclosure

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 (2025-09-09):	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.