SSA-999588: Multiple Vulnerabilities in User Management Component (UMC) Before V2.11.2

Publication Date: 2023-12-12
Last Update: 2024-10-08
Current Version: V1.6
CVSS v3.1 Base Score: 7.5

SUMMARY

Siemens User Management Component (UMC) before V2.11.2 is affected by multiple vulnerabilities where the most severe could lead to a restart of the UMC server.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Opcenter Execution Foundation: All versions < V2407 affected by all CVEs	Update to V2407 or later version https://support.sw.siemens.com/product/219646572/ See further recommendations from section Workarounds and Mitigations
Opcenter Quality: All versions < V2312 affected by all CVEs	Update to V2312 or later version https://support.sw.siemens.com/ See further recommendations from section Workarounds and Mitigations
SIMATIC PCS neo: All versions < V4.1 affected by all CVEs	Update to V4.1 or later version See further recommendations from section Workarounds and Mitigations
SINEC NMS: All versions < V2.0 SP1 affected by all CVEs	Update to V2.0 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109826954/ See further recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal):	See below See recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V14: All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations

Totally Integrated Automation Portal (TIA Portal) V15.1: All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V16: All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V17: All versions < V17 Update 8 affected by all CVEs	Update to V17 Update 8 or later version https://support.industry.siemens.com/cs/ww/en/view/109784441/ See further recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V18: All versions < V18 Update 3 affected by all CVEs	Update to V18 Update 3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817218/ 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-2023-46281, CVE-2023-46282: Do not access links from untrusted sources
- CVE-2023-46283, CVE-2023-46284: If only one UMC server is used, block access to port 4002/tcp e.g. with an external firewall
- CVE-2023-46284, CVE-2023-46285: If only one RT server is used, block access to port 4004/tcp e.g. with an external firewall. If the deployment contains no RT-Servers, block the port in the local firewall.

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

SIMATIC IT Unified Architecture Foundation (SIT UAF) is a framework to build and run state-of-the-art manufacturing operations management (MOM) applications.

Opcenter Quality is a quality management system (QMS) that enables organizations to safeguard compliance, optimize quality, reduce defect and rework costs and achieve operational excellence by increasing process stability. The integrated process capabilities (control charts, statistics, quality gates) can detect production errors to avoid further processing and shipment of nonconforming material.

SIMATIC PCS neo is a distributed control system (DCS).

SINEC NMS is a new generation of the Network Management System (NMS) for the Digital Enterprise. This system can be used to centrally monitor, manage, and configure networks.

SINUMERIK Integrate product suite facilitates simple networking of machine tools in the IT of the production landscape.

Totally Integrated Automation Portal (TIA Portal) is a PC software that provides access to the complete range of Siemens digitalized automation services, from digital planning and integrated engineering to transparent operation.

User Management Component (UMC) is an integrating component that enables system-wide, central maintenance of users.

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-2023-46281

When accessing the UMC Web-UI from affected products, UMC uses an overly permissive CORS policy. This could allow an attacker to trick a legitimate user to trigger unwanted behavior.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-942: Permissive Cross-domain Policy with Untrusted Domains

Vulnerability CVE-2023-46282

A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected applications that could allow an attacker to inject arbitrary JavaScript code. The code could be potentially executed later by another (possibly privileged) user.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2023-46283

The affected application contains an out of bounds write past the end of an allocated buffer when handling specific requests on port 4002/tcp. This could allow an attacker to crash the application. The corresponding service is auto-restarted after the crash.

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/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2023-46284

The affected application contains an out of bounds write past the end of an allocated buffer when handling specific requests on port 4002/tcp and 4004/tcp. This could allow an attacker to crash the application. The corresponding service is auto-restarted after the crash.

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/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2023-46285

The affected application contains an improper input validation vulnerability that could allow an attacker to bring the service into a Denial-of-Service state by sending a specifically crafted message to 4004/tcp. The corresponding service is auto-restarted after the crash is detected by a watchdog.

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/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

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 (2023-12-12):	Publication Date
V1.1 (2024-01-09):	Added fix for Totally Integrated Automation Portal (TIA Portal) V17
V1.2 (2024-02-13):	Added fix for Opcenter Quality as well as product and fix for SINEC NMS
V1.3 (2024-05-14):	Removed unaffected product SINUMERIK Integrate RunMyHMI /Automotive
V1.4 (2024-08-13):	Errata: Removed fix for Totally Integrated Automation Portal (TIA Portal) V17
V1.5 (2024-09-10):	Added fix for Totally Integrated Automation Portal (TIA Portal) V17
V1.6 (2024-10-08):	Added affected product and fix for Opcenter Execution Foundation

TERMS OF USE