مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Siemens User Management Component (UMC)

Tracking #:432316652

Date:20-12-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Siemens has disclosed a critical heap-based buffer overflow vulnerability in its User Management Component (UMC), affecting multiple industrial control system products.

TECHNICAL DETAILS:

Siemens has disclosed a critical heap-based buffer overflow vulnerability (CVE-2024-49775) in its User Management Component (UMC), affecting multiple industrial control system products.

Vulnerability Details

- CVE-2024-49775
- CVSS v3.1 Base Score:9.8 (Critical)
- A heap-based buffer overflow vulnerability which could allow an unauthenticated remote attacker arbitrary code execution.

Affected Versions:

- Opcenter Execution Foundation: All versions
- Opcenter Intelligence: All versions
- Opcenter Quality: All versions
- Opcenter RDL: All versions
- SIMATIC PCS neo: All versions (V4.0, V4.1, V5.0 prior to V5.0 Update 1)
- SINEC NMS: All versions
- Totally Integrated Automation Portal (TIA Portal): All versions (V16, V17, V18, V19)

Fixed Versions:

- SIMATIC PCS neo V5.0: Update to V5.0 Update 1 or later.
- SINEC NMS: Update to V3.0 SP2 or later, and UMC to V2.15 or later**.**
- For other affected products, refer to the official Siemens security advisory for patching and update information.

Mitigations:

- Network Filtering: Implement strict filtering on ports 4002 and 4004
- Port Blocking: Block port 4004 if not using RT server machines
- Environment Hardening: Configure the IT environment according to Siemens' operational guidelines for industrial security

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions or mitigate this critical vulnerability at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://cert-portal.siemens.com/productcert/html/ssa-928984.html