مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Access Control Vulnerability in Verve Asset Manager

Tracking #:432318006

Date:14-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical severity access control vulnerability has been identified in Verve Asset Manager.

TECHNICAL DETAILS:

A critical severity access control vulnerability (CVE-2025-11862) has been identified in Verve Asset Manager, an operational technology (OT) cybersecurity platform widely used for asset visibility, vulnerability management, and automated security operations.

The flaw could allow unauthorized read-only users to read, update, or delete user information through the platform's API, potentially leading to unauthorized user management or privilege escalation within OT environments.

Vulnerability Details

- CVE ID: CVE-2025-11862
- Vulnerability Type: Incorrect Authorization (CWE-863)
- CVSS v3.1 Base Score: 9.9 (Critical)
- CVSS v4.0 Base Score: 8.4 (High)
- Impact:
  - Allows unauthorized read-only users to read, modify, or delete user accounts through the API.
  - Compromises access control integrity and may enable privilege escalation or denial of service within the management console.
- Affected Product: Verve Asset Manager
- Affected Versions: 1.33 to 1.41.3
- Patched Versions: 1.41.4 and 1.42

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade Verve Asset Manager to a patched version immediately.

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://www.rockwellautomation.com/en-us/trust-center/security advisories/advisory.SD1759.html