مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Flaws in Rockwell Arena Simulation

Tracking #:432317570

Date:06-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple high-severity memory abuse vulnerabilities in Rockwell Automation's Arena Simulation software, which could be exploited through malicious files or webpages.

TECHNICAL DETAILS:

The vulnerabilities arise from improper memory handling in Arena Simulation. When a user opens a specially crafted file or webpage, the software may read or write beyond allocated memory boundaries. This can lead to:

- Execution of arbitrary code
- Leakage of sensitive data from memory

These issues are particularly concerning in environments where Arena is used for modeling critical systems in manufacturing, healthcare, and supply chains.

Vulnerability Details:

- **Vulnerability IDs:** CVE-2025-7025, CVE-2025-7032, CVE-2025-7033
- **Severity:** High
- **CVSS v3.1 Score:** 7.8
- **Type:** Memory Corruption / Abuse
- **Impact:** Remote Code Execution, Information Disclosure
- **Attack Vector:** Maliciously crafted file or webpage
- **User Interaction Required:** Yes

Affected Versions

- Arena Simulation: Version 16.20.09 and earlier

Fixed Version

- Arena Simulation: Version 16.20.10 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed updates released by the Vendor.

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.SD1731.html