مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Johnson Controls ICU Tool

Tracking #:432317326

Date:29-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the Johnson Controls iSTAR Configuration Utility (ICU) tool, which could be exploited to gain access to sensitive data from the memory of the Windows PC running the ICU tool.

TECHNICAL DETAILS:

A vulnerability has been identified in the Johnson Controls iSTAR Configuration Utility (ICU) tool, affecting all versions prior to 6.9.5. This vulnerability, if exploited, could allow an attacker to access sensitive data from the memory of the Windows PC running the ICU tool.

Vulnerability Details:

- **CVE-2025-26383**
- **CVSS v3.1 Base Score:** 7.4 (High)
- The ICU tool leaks memory due to the use of an uninitialized variable. An attacker with network access could exploit this flaw to obtain sensitive information from the host system's memory. This vulnerability only affects the ICU tool and the Windows PC it is running on. It does not impact iSTAR controllers, including legacy, Ultra, and G2 series.

Affected Versions:

- ICU Tool: All versions prior to 6.9.5

Fixed Versions:

- ICU tool version 6.9.5 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Johnson Controls.

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.johnsoncontrols.com/trust-center/cybersecurity/security-advisories