

Forum:[Hack Forums](#)

Thread: [Johnson Controls Inc. iSTAR Configuration Utility \(ICU\) tool](#)

Stanley - February 6, 2026, 4:35 am

Johnson Controls Inc. iSTAR Configuration Utility (ICU) tool

View CSAF

Summary

Successful exploitation of this vulnerability could allow an attacker to cause a failure within the operating system of the machine hosting the ICU tool.

The following versions of Johnson Controls Inc. iSTAR Configuration Utility (ICU) tool are affected:

iSTAR Configuration Utility (ICU) tool (CVE-2025-26386)

CVSS

Vendor

Equipment

Vulnerabilities

v3 7.1

Johnson Controls Inc.

Johnson Controls Inc. iSTAR Configuration Utility (ICU) tool

Stack-based Buffer Overflow

Background

Critical Infrastructure Sectors: Commercial Facilities, Critical Manufacturing, Energy, Government Services and Facilities, Transportation Systems

Countries/Areas Deployed: Worldwide

Company Headquarters Location: Ireland

Vulnerabilities

Expand All +

CVE-2025-26386

Under certain circumstances, a successful exploitation of this vulnerability could result in failure

within the operating system of the machine hosting the ICU tool.

View CVE Details

Affected Products

Johnson Controls Inc. iSTAR Configuration Utility (ICU) tool

Vendor:Johnson Controls Inc.

Product Version:Johnson Controls Inc. iSTAR Configuration Utility (ICU) tool: <=6.9.7

Product Status:known_affected

Remediations

MitigationJohnson Controls Inc. recommends the following:

Vendor fixUpdate the iSTAR Configuration Utility (ICU) tool to version 6.9.8

MitigationFor more detailed mitigation instructions, please see Johnson Controls Product Security Advisory JCI-PSA-2025-08 v1 at the following location:

<https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories>

Relevant CWE: CWE-121 Stack-based Buffer Overflow

Metrics

CVSS Version

Base Score

Base Severity

Vector String

3.1

7.1

HIGH

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:H

Acknowledgments

Tenable reported this vulnerability to CISA

Legal Notice and Terms of Use

This product is provided subject to this Notification (<https://www.cisa.gov/notification>) and this Privacy & Use policy (<https://www.cisa.gov/privacy-policy>).

Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability, such as:

- Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.
- Locate control system networks and remote devices behind firewalls and isolating them from business networks.
- When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.
- CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.
- CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov/ics. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.
- CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.
- Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.
- Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.
- CISA also recommends users take the following measures to protect themselves from social engineering attacks:
 - Do not click web links or open attachments in unsolicited email messages.
 - Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.
 - Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.
- No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time.

Revision History

Initial Release Date: 2026-01-22

Date
Revision
Summary

2026-01-22
1
Initial Publication

Legal Notice and Terms of Use

<https://www.cisa.gov/news-events/ics-advisories/icsa-26-022-04>