OpenBlue
Trust Center

Johnson Controls

Product Security Advisory

April 24, 2025

JCI-PSA-2024-06-v2
CVE-2024-32752
ICSA-24-158-04

Note

This Product Security Advisory (PSA) updates a previously published CVE (CVE-2024-32752 / JCI-PSA-2024-06), providing additional clarity to the original information.

Overview

Johnson Controls has confirmed a vulnerability impacting the Software House iSTAR Configuration Utility (ICU) tool for Software House iSTAR Pro, Edge, eX, Ultra and Ultra LT door controllers which may result in insecure communications.

Impact

The iSTAR door controllers running firmware prior to version 6.6.B, does not support authenticated communications with ICU, which may allow an attacker to gain unauthorized access.

Affected Versions

- iSTAR Pro, Edge and eX all versions
- iSTAR Ultra all versions prior to 6.6.B
- iSTAR Ultra LT all versions prior to 6.6.B
- ICU all versions

Mitigation

- Replace the iSTAR Pro, Edge and eX door controllers with a current generation iSTAR door controller (such as iSTAR Ultra G2) which supports authentication and prevents the ICU from making configuration changes.
- Ensure your iSTAR Ultra and Ultra LT door controllers are running firmware 6.6.B or greater.

Initial Publication Date

June 6, 2024

Last Published Date

April 24, 2025

Resources

Cyber Solutions Website - https://www.johnsoncontrols.com/cyber-solutions/security-advisories
CVE-2024-32752 - NIST National Vulnerability Database (NVD) and CVE®
ICSA-24-158-04 - CISA ICS-CERT Advisories

Trust Center