Product Security Advisory

June 6, 2024

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

Overview

Johnson Controls has confirmed a vulnerability impacting Software House iSTAR Pro door controllers.

Impact

Under certain circumstances communications between the ICU tool and iSTAR Pro door controller is susceptible to Machine-in-the-Middle attacks which could impact door control and configuration.

Affected Versions

- iSTAR Pro (all versions)
- ICU (all versions)

Mitigation

- The iSTAR Pro controller has reached its end-of-support period and no further firmware updates will be provided. However, the iSTAR Pro has a physical dip switch located on its GCM board, labeled S4, that can be configured to block out communications to the ICU tool. Please consult the iSTAR Pro Installation and Configuration Guide for more details on how to set the dip switch to mitigate this vulnerability.

Publication Date

June 06, 2024

Last Published Date

June 06, 2024

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