Product Security Advisory

August 13, 2025

JCI-PSA-2025-10
CVE-2025-53695
CVE-2025-53696
CVE-2025-53697
CVE-2025-53698
CVE-2025-53699
CVE-2025-53700
ICSA-25-224-02

Overview

Johnson Controls has identified a set of previously undiscovered vulnerabilities affecting the following door controller models: Software House iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE, and iSTAR Edge G2

- OS Command Injection
- Insufficient Verification of Data Authenticity
- Use of Default Credentials
- Mechanism for Alternate Hardware Interface - Physical Serial Access
- Mechanism for Alternate Hardware Interface - Physical USB Access
- Insecure Storage of Sensitive Information

Note: Johnson Controls made firmware version 6.9.3 available in 2024 to fix CVE-2025-53695 and lower the risk of exploitation for CVE-2025-53696, CVE-2025-53697 and CVE-2025-53700; the other two vulnerabilities require direct physical access to the controller.

CVE-2025-53695

Johnson Controls has confirmed a vulnerability impacting Software House iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE and iSTAR Edge G2 door controllers which may allow an authenticated attacker to gain privileged access (‘root’ user) to the device firmware.

Impact

Under certain circumstances the web application for iSTAR Ultra, Ultra SE, Ultra G2, Ultra G2 SE and iSTAR Edge G2 door controllers may allow an authenticated attacker to gain privileged access ('root' user) to the device firmware.

Affected Versions

- iSTAR Ultra for versions 6.9.2.CU02 and prior
- iSTAR Ultra SE for versions 6.9.2.CU02 and prior
- iSTAR Ultra G2 for versions 6.9.2.CU02 and prior

- iSTAR Ultra G2 SE for versions 6.9.2.CU02 and prior
- iSTAR Edge G2 for versions 6.9.2.CU02 and prior

Mitigation
Upgrade iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE and iSTAR Edge G2 to version 6.9.3 or higher. In addition, we strongly recommend disabling the web server on iSTAR after initial installation, according to the hardening guide.

CVE-2025-53696
Johnson Controls has confirmed a vulnerability impacting Software House iSTAR Ultra and Ultra SE door controllers which may allow lack of firmware tamper detection/out of band changes.

Impact
iSTAR Ultra and iSTAR Ultra SE, versions 6.9.2.CU02 and prior perform a firmware verification on boot, however the verification does not inspect certain portions of the firmware. These can be exploited via OS command injection described in CVE-2025-53695 as an authenticated user.

Affected Versions
- iSTAR Ultra for versions 6.9.2.CU02 and prior
- iSTAR Ultra SE for versions 6.9.2.CU02 and prior

Mitigation
iSTAR Ultra and iSTAR Ultra SE door controllers should be updated to version 6.9.3 or higher to ensure protection against command injection as described in **CVE-2025-53695**. In addition, we strongly recommend disabling the web server on iSTAR after initial installation, according to the hardening guide.

CVE-2025-53697
Johnson Controls has confirmed a vulnerability impacting Software House iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE and iSTAR Edge G2 door controllers which may allow an authenticated attacker to gain OS command access to a controller.

Impact
Under certain circumstances, when an attacker can leverage command injection as described in **CVE-2025-53695** to access an iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE and iSTAR Edge G2 door controller, it may be possible to utilize a default root password which can be changed through the command shell.

Affected Versions
- iSTAR Ultra for versions 6.9.2.CU02 and prior
- iSTAR Ultra SE for versions 6.9.2.CU02 and prior
- iSTAR Ultra G2 for versions 6.9.2.CU02 and prior
- iSTAR Ultra G2 SE for versions 6.9.2.CU02 and prior
- iSTAR Edge G2 for versions 6.9.2.CU02 and prior

Mitigation
iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE and iSTAR Edge G2 door controllers should be updated to version 6.9.3 or higher to ensure protection against command injection as described in **CVE-2025-53695**. In addition, we strongly recommend disabling the web server on iSTAR after initial installation, according to the hardening guide.

CVE-2025-53698
Johnson Controls has confirmed a vulnerability impacting Software House iSTAR Ultra and iSTAR Ultra SE door controllers which may allow an attacker to gain physical serial console access.

Impact
Under certain circumstances, when an attacker can gain physical access to an iSTAR Ultra and iSTAR Ultra SE door controllers, it may be possible to access the iSTAR GCM (General Controller Module) serial console which provides access to Uboot.

Affected Versions
- iSTAR Ultra all versions
- iSTAR Ultra SE all versions

Mitigation
Ensure physical access to iSTAR Ultra and iSTAR Ultra SE door controller is limited to authorized personnel. Door controllers should be installed in a locked enclosure with physical tamper switch per industrial standards and as indicated in the installation manual and hardening guide.

CVE-2025-53699
Johnson Controls has confirmed a vulnerability impacting Software House iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE, and iSTAR Edge G2 door controllers, if an attacker gains physical access to the door controller it may be possible to access a USB console.

Impact
Under certain circumstances, when an attacker can gain physical access to an iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE and iSTAR Edge G2 door controller, it may be possible to access a USB console on the controller board.

Affected Versions
- iSTAR Ultra all versions
- iSTAR Ultra SE all versions
- iSTAR Ultra G2 all versions
- iSTAR Ultra G2 SE all versions
- iSTAR Edge G2 all versions

Mitigation
Ensure physical access to iSTAR Ultra door controller is limited to authorized personnel. Door controllers should be installed in a locked enclosure with physical tamper switch per industrial standards and as indicated in the installation manual and hardening guide.

CVE-2025-53700
Johnson Controls has confirmed a vulnerability impacting Software House iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE, and iSTAR Edge G2 door controllers where a firmware signing key can be accessed by an authenticated user by exploiting OS command injection in CVE-2025-53695.

Impact
Under certain circumstances, when an attacker can gain access to iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE, and iSTAR Edge G2 door controllers, versions 6.9.2.CU02 and prior, it may be possible to access a firmware signing key used with other products.

Affected Versions
- iSTAR Ultra versions 6.9.2.CU02 and prior
- iSTAR Ultra SE versions 6.9.2.CU02 and prior
- iSTAR Ultra G2 versions 6.9.2.CU02 and prior
- iSTAR Ultra G2 SE versions 6.9.2.CU02 and prior
- iSTAR Edge G2 versions 6.9.2.CU02 and prior

Mitigation
iSTAR Ultra, iSTAR Ultra SE, iSTAR Ultra G2, iSTAR Ultra G2 SE, and iSTAR Edge G2 door controllers should be updated to version 6.9.3 or higher to ensure protection against command injection as described in **CVE-2025-53695**. In addition, we strongly recommend disabling the web server on iSTAR after initial installation, according to the hardening guide.

Initial Publication Date
August 13, 2025

Last Published Date
August 13, 2025

Resources
Cyber Solutions Website - https://www.johnsoncontrols.com/cyber-solutions/security-advisories
CVE-2025-53695 - NIST National Vulnerability Database (NVD) and CVE®
CVE-2025-53696 - NIST National Vulnerability Database (NVD) and CVE®
CVE-2025-53697- NIST National Vulnerability Database (NVD) and CVE®
CVE-2025-53698 - NIST National Vulnerability Database (NVD) and CVE®
CVE-2025-53699 - NIST National Vulnerability Database (NVD) and CVE®
CVE-2025-53700 - NIST National Vulnerability Database (NVD) and CVE®
ICSA-25-224-02 - CISA ICS-CERT Advisories

In addition to the guidance provided in this advisory, the recommendation provided within Johnson Controls Hardening Guide should always be applied to minimize security risk.

Visit the Johnson Controls Trust Center Cybersecurity website to access the latest Hardening Guidelines and best practice in cybersecurity - https://www.johnsoncontrols.com/trust-center/cybersecurity/resources.

Trust Center Cybersecurity
Johnson Controls