CISA flags cleartext transmission flaw in Johnson Controls EasyIO Neo EC and CW controllers



CISA published an advisory on CVE-2026-64893 in Johnson Controls EasyIO Neo EC and CW controllers. Sensitive data, including credentials and session data, may be sent in cleartext and read by an attacker on the network.

- The issue is tracked as CVE-2026-64893 and is classed as cleartext transmission of sensitive information.
- CVSS v3 score is 5.4.
- Affected: EasyIO Neo EC controllers V3.3b62 and V3.3b63, and CW controllers V3.3b24 and V3.3b25.
- An attacker able to intercept network traffic could read credentials and session data.
- CISA lists sectors including critical manufacturing, commercial facilities, government facilities,

> transportation and energy.

CISA has published an industrial control systems advisory covering the Johnson Controls EasyIO Neo Series EC and CW controllers. The flaw, CVE-2026-64893, concerns the transmission of sensitive information in cleartext over the network.

What the advisory says

Johnson Controls is aware that an attacker could intercept and read information sent unencrypted, including credentials and session data. The advisory rates the issue at CVSS v3 5.4.

The affected versions are:

- EasyIO Neo Series EC Controllers V3.3b62 and V3.3b63
- EasyIO Neo Series CW Controllers V3.3b24 and V3.3b25

CISA associates the product with critical manufacturing, commercial facilities, government services and facilities, transportation systems and energy. The vendor is headquartered in Ireland and the products are deployed worldwide.

Why it matters

The score is moderate, but captured credentials or session data could give an attacker a foothold in building or facility control systems. Exposure depends on whether an attacker can reach the network path between users and the controllers.

Next steps

Operators should first identify whether these controllers are in their estate and which versions they run. They should then follow the vendor's guidance and CISA's advisory for remediation, and review how the controllers are reached on the network. The source excerpt does not describe a patch or workaround, so confirm current guidance directly with Johnson Controls.

What to do now

1. Inventory EasyIO Neo EC and CW controllers and record their firmware versions against the affected list.
2. Check Johnson Controls and the CISA advisory for current remediation guidance and apply it.
3. Restrict network access to the controllers to segmented management networks and trusted hosts only.
4. Rotate credentials used on affected controllers if exposure on an untrusted network is possible.
5. Monitor traffic to and from the controllers for unexpected sessions or logins.