

Johnson Controls EasyIO FG Building Controllers Contain Hard-Coded Credentials and Privilege Management Flaws



CISA warns that Johnson Controls EasyIO FG building automation controllers contain hard-coded credentials and privilege management vulnerabilities that could allow full device compromise.

- Two vulnerabilities (CVE-2026-27872, CVE-2026-27873) affect EasyIO FG firmware version 2.0b52 and earlier
- Hard-coded credentials and improper privilege management could enable full unauthorized device access
- CVSS score of 7.7 indicates high severity impact on operational technology environments
- Johnson Controls has declared the EasyIO FG Series end-of-life with no security patches planned
- Affected systems are deployed in critical manufacturing, commercial facilities, government

Vulnerability Overview

The US Cybersecurity and Infrastructure Security Agency has published an advisory concerning two vulnerabilities in Johnson Controls EasyIO FG building automation controllers. The flaws, tracked as CVE-2026-27872 and CVE-2026-27873, affect all firmware versions up to and including 2.0b52. Both vulnerabilities stem from the use of **hard-coded credentials** and **improper privilege management**, enabling an attacker to gain full unauthorized access to affected devices. CISA has assigned a CVSS score of 7.7, reflecting the potential for significant technical and operational impact.

The EasyIO FG series is deployed globally across critical infrastructure sectors including critical manufacturing, commercial facilities, government services, transportation systems, and energy. These building automation controllers manage HVAC, lighting, and other facility systems, making them attractive targets for adversaries seeking to disrupt operations or establish persistence in operational technology environments.

End-of-Life Status and No Patch Available

Johnson Controls has determined that the EasyIO FG Series has reached end-of-life status. As a result, the vendor will not release security patches to address these vulnerabilities. Organizations relying on these controllers face a choice between accepting the risk, implementing compensating controls, or replacing the affected hardware with supported alternatives.

Risk to Saudi Regulated Institutions

For institutions operating under National Cybersecurity Authority frameworks or SAMA regulations, the presence of unpatched vulnerabilities in operational technology environments represents a compliance and operational risk. Building automation systems often bridge IT and OT networks, and compromise of these devices could provide attackers with lateral movement opportunities or enable disruption of critical facility operations.

What to do now

1. Conduct an immediate inventory of all Johnson Controls EasyIO FG controllers across your facilities and document firmware versions
2. Isolate affected devices on dedicated network segments with strict firewall rules preventing direct internet access and limiting lateral movement
3. Implement enhanced monitoring and logging for all EasyIO FG devices to detect unauthorized access attempts or configuration changes
4. Develop and execute a replacement roadmap for end-of-life EasyIO FG controllers, prioritizing devices in critical infrastructure or high-security zones

5. Review and update building automation system security controls in line with NCA OTCC requirements for operational technology environments
6. Brief facility management and operational technology teams on the vulnerability and interim security measures until replacement is complete