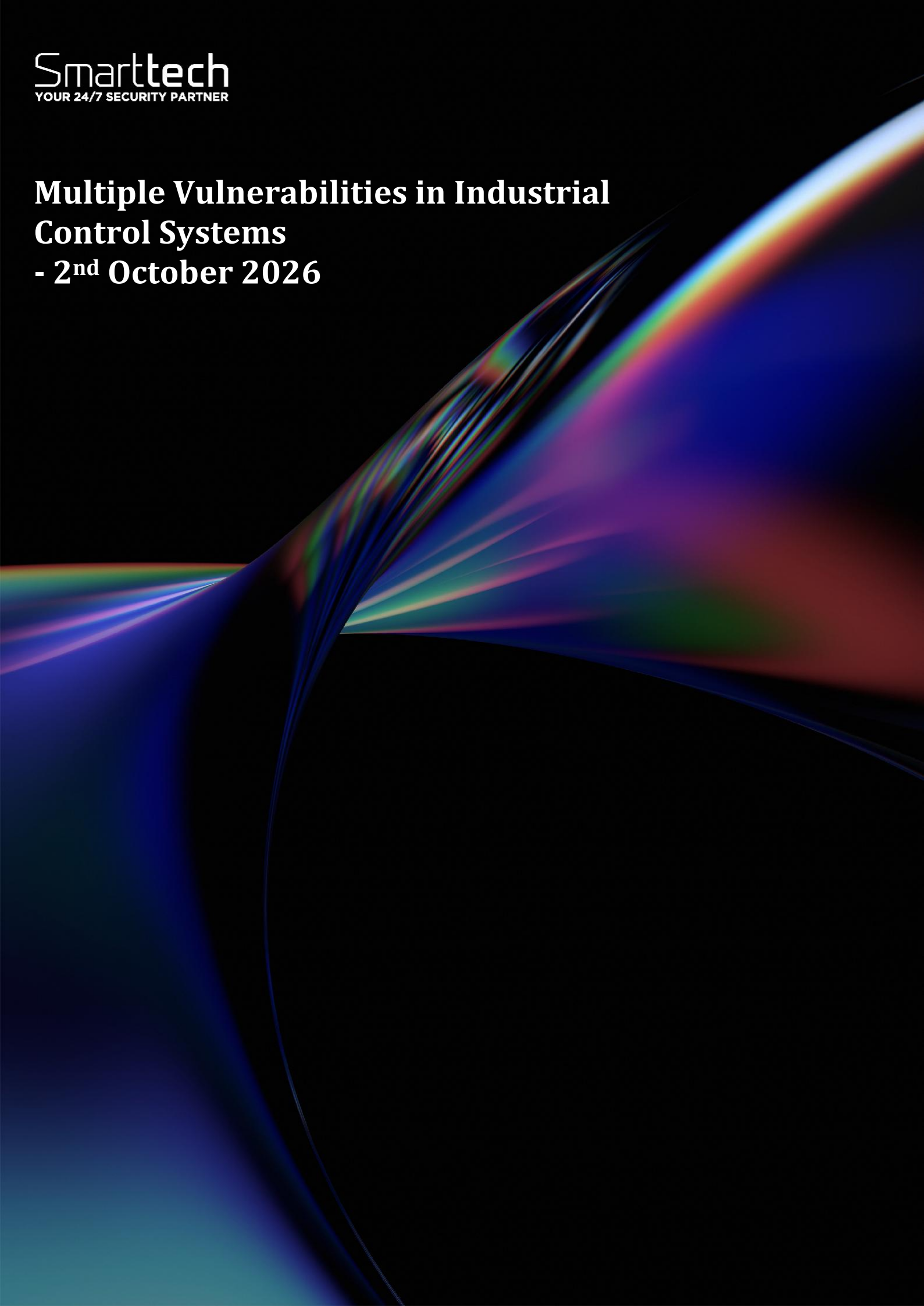


Multiple Vulnerabilities in Industrial Control Systems

- 2nd October 2026



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	173
Authors	Alex Ciuta < alexandru.ciuta@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-02
Issue Date	2026-10-02

This document and any information therein are confidential property of Smarttech247 and without infringement neither the whole nor any extract may be disclosed, loaned, copied or used for manufacturing, provision of services or other purposes whatsoever without prior written consent of Smarttech247, and no liability is accepted for loss or damage from any cause whatsoever from the use of the document. Smarttech247 retain the right to alter the document at any time unless a written statement to the contrary has been appended.

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released.

Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

Multiple vulnerabilities have been identified in the following CISA Malcolm, Meari IoT Cloud Platform OpenAPI Service, Johnson Controls EasyIO Neo Series EC and CW Controllers, ABB Protection and Control IED Manager PCM600, Monta monta.app, and Armatura LLC Armatura One. Successful exploitation of the vulnerabilities addressed in these advisories could allow attackers to execute arbitrary code, escalate privileges, gain unauthorized access to sensitive information and devices, manipulate system configurations, bypass authentication and authorization controls, overwrite files, or cause denial-of-service conditions on affected systems.

Armatura LLC Armatura One

Summary

Successful exploitation of these vulnerabilities could allow an attacker to gain unauthorized access to the database, execute arbitrary code on the host with the highest level of privilege, or gain control of the physical access-control system.

The following versions of **Armatura LLC Armatura One** are affected:

- **Armatura One <4.7.2 (CVE-2023-46604, CVE-2026-94591, CVE-2026-94592, CVE-2026-94593, CVE-2026-94594)**
- **Armatura One (USA) <4.6.1 (CVE-2023-46604, CVE-2026-94591, CVE-2026-94592, CVE-2026-94593, CVE-2026-94594)**
- **CVSS v3 9.8**
- **Vendor:** Armatura LLC
- **Equipment:** Armatura LLC, Armatura One
- **Vulnerabilities:** Deserialization of Untrusted Data, Use of Hard-coded Cryptographic Key, Use of Hard-coded Credentials, Insertion of Sensitive Information into Log File

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2023-46604	Critical	Armatura One embeds Apache ActiveMQ, exposing its OpenWire protocol listener on the network by default. This embedded version is affected by CVE-2023-46604, a deserialization flaw in the OpenWire marshaller that allows an unauthenticated network

		attacker to trigger deserialization of an arbitrary object graph before authentication is checked. This can result in arbitrary code execution with the highest level of privilege on the host operating system.
CVE-2026-94591	High	Armatura One stores database and message-broker credentials in an install configuration file, encrypting them with AES-128-CBC when this protection is enabled. The encryption key and initialization vector are fixed values embedded in the software itself and are identical across every installation. An attacker with a copy of the installation package can recover this key and initialization vector, and can then decrypt the stored credentials of any specific installation to which the attacker separately obtains the encrypted configuration file.
CVE-2026-94592	High	Armatura One's database initialization routine assigns a fixed, vendor-defined password to the database superuser account at creation time, rather than generating a unique password per installation. An individual with access to the server operating system and knowledge of this value can authenticate as the database superuser on a deployment where it has not been changed.
CVE-2026-94593	High	Armatura One's backup and restore routine records the full database connection command, including the superuser password, in plain text in a log file on the host. Credentials disclosed by this finding can be used to access the database when access to the server operating system is available.
CVE-2026-94594	Medium	Armatura One's message broker logs client connection credentials and the associated password in plain text during normal operation. Any party with read access to this log, or to a backup or support bundle that includes it, can obtain the logged credential.

Remediation:

- Armatura LLC Armatura One vers:all/<4.7.2: Armatura LLC has released Armatura One V4.7.2, which resolves this issue. Users should upgrade from V4.7.1 or earlier to V4.7.2.
- Armatura LLC Armatura One (USA) vers:all/<4.6.1: Armatura LLC has released Armatura One V4.6.1_USA, which resolves this issue. Users of the USA release line should upgrade from V4.3.1_USA or earlier to V4.6.1_USA.
- Armatura LLC recommends contacting official technical support for guidance on obtaining and applying the upgrade.

Monta monta.app

Summary

Successful exploitation of these vulnerabilities could enable attackers to gain unauthorized administrative control over vulnerable charging stations or disrupt charging services through denial-of-service attacks.

The following versions of **Monta monta.app** are affected:

- **monta.app vers:all/* (CVE-2026-95102, CVE-2026-97363, CVE-2026-97212, CVE-2026-93474)**
- **CVSS v3 9.4**
- **Vendor: Monta**

- **Equipment:** Monta monta.app
- **Vulnerabilities:** Missing Authentication for Critical Function, Improper Restriction of Excessive Authentication Attempts, Insufficient Session Expiration, Insufficiently Protected Credentials

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-95102	Critical	WebSocket endpoints lack proper authentication mechanisms, enabling attackers to impersonate charging stations. As a result, attackers can exploit this weakness to gain unauthorized access to sensitive data or perform unauthorized actions. Given that no authentication is required, this can lead to privilege escalation and potentially compromise the security of the entire system.
CVE-2026-97363	High	The WebSocket Application Programming Interface lacks restrictions on the number of authentication requests. This absence of rate limiting may allow an attacker to conduct denial-of-service attacks or brute-force attacks to gain unauthorized access.
CVE-2026-97212	High	The WebSocket backend uses charging station identifiers to uniquely associate sessions but allows multiple endpoints to connect using the same session identifier. This implementation results in predictable session identifiers. This vulnerability may allow unauthorized users to authenticate as other users or enable a malicious actor to cause a denial-of-service condition by overwhelming the backend with valid session requests.
CVE-2026-93474	Medium	Charging station authentication identifiers are publicly accessible via web-based mapping platforms.

Mitigation:

- Monta states that they are actively working to increase adoption of authenticated connections across their network and to deprecate unauthenticated access on a rolling basis. Monta states that they provide support for OCPP 1.6 Security Profile 2 (HTTP Basic Auth with TLS) and encourage operators to enable it.
- Monta states that they have implemented rate limiting and automated connection throttling at the WebSocket layer. Connections exhibiting abusive patterns, including rapid reconnection, ID brute-forcing behavior, or excessive command volume, are automatically identified and blocked.
- Monta states that their platform handles duplicate connection attempts per the OCPP specification, where a new authenticated connection supersedes an existing session for the same station ID.

ABB Protection and Control IED Manager PCM600

Summary

Successful exploitation of these vulnerabilities could allow an attacker to escalate privileges or overwrite files.

The following versions of **ABB Protection and Control IED Manager PCM600** are affected:

- **Protection and Control IED Manager PCM600 <=2.14 (CVE-2026-15952, CVE-2026-15953)**

- **CVSS v3 6.4**
- **Vendor:** ABB
- **Equipment:** ABB Protection and Control IED Manager PCM600
- **Vulnerabilities:** Incorrect Permission Assignment for Critical Resource, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-15952	Medium	A vulnerability exists in the Scheduler Service installed with PCM600. The service executes under the LocalSystem account while permissions are granted to standard PCM600 users through membership in the local users group. An attacker with local access and valid user credentials may exploit this vulnerability to elevate privileges and obtain control of the affected host.
CVE-2026-15953	Medium	A vulnerability exists in the processing of PCM600 project archives files. Insufficient validation of archive entry paths may permit path traversal during extraction, potentially allowing files to be written to locations outside the intended extraction directory.

Mitigation:

- Configure the appropriate ABBPCMSchedulerService instance to run using the same Windows account that is used to operate PCM600:
 - Open Services.msc.
 - Locate the ABBPCMSchedulerService corresponding to the installed PCM600 version.
 - Open Properties and select the Log On tab.
 - The service should be configured to log on with the same Windows user account that is used for the PCM600 application.
 - Ensure that this account has the required "Log on as a service" privilege.
- When authentication is enabled for the IED, the Scheduler tool must be used with the same Windows account configured as the Scheduler Service logon account.
- For installations using IED security certificates, the PCM600 setting Always trust IED security certificates must be enabled only when PCM600-to-IED communication takes place in a secure and trusted environment.

Johnson Controls EasyIO Neo Series EC and CW Controllers

Summary

Successful exploitation of this vulnerability could allow an attacker to gain access to sensitive information that could be used to conduct further attacks against the system.

The following versions of **Johnson Controls EasyIO Neo Series EC and CW Controllers** are affected:

- **EasyIO Neo Series EC Controllers V3.3b63 (CVE-2026-64892)**
- **EasyIO Neo Series EC Controllers V3.3b62 (CVE-2026-64892)**
- **EasyIO Neo Series CW Controllers V3.3b25 (CVE-2026-64892)**
- **EasyIO Neo Series CW Controllers V3.3b24 (CVE-2026-64892)**
- **CVSS v3 3.5**
- **Vendor:** Johnson Controls
- **Equipment:** Johnson Controls EasyIO Neo Series EC and CW Controllers

- **Vulnerabilities:** Exposure of Sensitive Information to an Unauthorized Actor

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-64892	Medium	Johnson Controls is aware of a vulnerability in EasyIO Neo Series EC and CW Controllers relating to an attacker gaining access to sensitive information that could be used to conduct further attacks against the system. The EC and CW are programmable edge controllers designed for building automation and control systems, used to manage and automate various building functions including HVAC, lighting, and energy management, supporting open protocols such as BACnet and Modbus for adaptable system connections.

Mitigation:

- Johnson Controls released fixed versions for EasyIO Neo Series EC and CW Controllers. Users should upgrade to the fixed version or later as soon as operationally feasible. The fix is available in EC firmware V3.3b64 and CW firmware V3.3b26. Contact your Johnson Controls representative or authorized EasyIO distributor.
- Before applying updates in production ICS/OT environments, users should review operational impact, backup relevant configurations, test updates in a non-production environment where feasible, and follow applicable change-management and safety procedures.
- If immediate update is not possible, Johnson Controls recommends the following mitigations:
 - Implement physical access controls to prevent unauthorized personnel from reaching device debug ports.
 - Monitor network traffic to and from affected devices for unusual or unauthorized access attempts.
 - Apply the principle of least privilege to all accounts and services that interact with the affected devices.
 - Where possible, apply firmware updates that disable debug interfaces or require authentication before granting debug access.
 - Implement intrusion detection/prevention systems to monitor for exploitation attempts.
 - Refer to and follow all steps in the product hardening guide or the JCI universal hardening guide found here: <https://www.johnsoncontrols.com/trust-center/cybersecurity/resources>.
- These mitigations reduce risk but may not fully remediate the vulnerability. Users should update to the fixed versions when operationally feasible.

Johnson Controls EasyIO Neo Series EC and CW Controllers

Summary

Successful exploitation of this vulnerability could allow an attacker to intercept and read sensitive information, including credentials and session data.

The following versions of **Johnson Controls EasyIO Neo Series EC and CW Controllers** are affected:

- **EasyIO Neo Series EC Controllers V3.3b62 (CVE-2026-64893)**
- **EasyIO Neo Series EC Controllers V3.3b63 (CVE-2026-64893)**
- **EasyIO Neo Series CW Controllers V3.3b24 (CVE-2026-64893)**

- **EasyIO Neo Series CW Controllers V3.3b25 (CVE-2026-64893)**
- **CVSS v3 5.4**
- **Vendor:** Johnson Controls
- **Equipment:** Johnson Controls EasyIO Neo Series EC and CW Controllers
- **Vulnerabilities:** Cleartext Transmission of Sensitive Information

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-64893	Medium	Johnson Controls is aware of a vulnerability in EasyIO Neo which may allow an attacker to intercept and read sensitive information, including credentials and session data, transmitted in cleartext over the network. Successful exploitation could result in technical or operational impact. EasyIO Neo is a programmable building automation edge controller used to manage and automate HVAC, lighting, and energy systems in commercial buildings through a web-based interface.

Mitigation:

- Johnson Controls released fixed versions for EasyIO Neo Series EC and CW Controllers. Users should upgrade to the fixed version or later as soon as operationally feasible. HTTP communication has been disabled by default in the latest version. The fix is available in EC firmware V3.3b64 and CW firmware V3.3b26. Contact your Johnson Controls representative or visit the Johnson Controls Trust Center.
- Before applying updates in production ICS/OT environments, users should review operational impact, backup relevant configurations, test updates in a non-production environment where feasible, and follow applicable change-management and safety procedures.
- If immediate update is not possible, Johnson Controls recommends the following mitigations:
 - Enable and enforce HTTPS/TLS for all web-based management access to the device.
 - Disable HTTP access entirely.
 - Place devices on an isolated, segmented network behind a firewall to limit exposure of management interfaces.
 - Use a VPN when accessing devices remotely to encrypt all traffic in transit.
 - Monitor network traffic for unencrypted sensitive data leaving the management interface.
 - Restrict network access to management interfaces using access control lists (ACLs) to only trusted hosts. Refer to and follow all steps in the product hardening guide or the JCI universal hardening guide found here: <https://www.johnsoncontrols.com/trust-center/cybersecurity/resources>.
- These mitigations reduce risk but may not fully remediate the vulnerability. Users should update to the fixed versions when operationally feasible.
- Users should review logs, network telemetry, device events, and security monitoring tools for activity involving EasyIO NEO versions EC and CW. Relevant detection information may include: Unencrypted HTTP traffic to or from the device management interface on port 80. Network captures showing cleartext credentials or session tokens in HTTP requests. Unexpected devices or IP addresses accessing the web management console. ARP spoofing or other man-in-the-middle indicators on the local network segment. Unauthorized configuration changes that may indicate credential interception.
- The recommendations 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 cybersecurity best practices -

<https://www.johnsoncontrols.com/trust-center/cybersecurity/resources>.

- For more detailed mitigation instructions, please see Johnson Controls Product Security Advisory JCI-PSA-2026-30. - <https://www.johnsoncontrols.com/trust-center/cybersecurity/security-advisories>

Meari IoT Cloud Platform OpenAPI Service

Summary

Successful exploitation of these vulnerabilities could allow attackers to manipulate device configurations, trigger unauthorized behaviors, and access sensitive information such as device credentials, owner details, and network data without proper authorization.

The following versions of **Meari IoT Cloud Platform OpenAPI** are affected:

- **IoT Cloud Platform OpenAPI Service vers:all/* (CVE-2026-101104, CVE-2026-96613)**
- **CVSS v3 7.7**
- **Vendor:** Meari
- **Equipment:** Meari IoT Cloud Platform OpenAPI Service
- **Vulnerabilities:** Missing Authorization

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-101104	High	The Meari IoT Cloud Platform OpenAPI Service is vulnerable to an authorization flaw that allows authenticated users to manipulate the configurations of devices they do not own. This vulnerability enables attackers to perform unauthorized actions, such as altering device settings or triggering unintended behaviors, without verifying ownership or permissions.
CVE-2026-96613	High	The Meari IoT Cloud Platform OpenAPI Service is vulnerable to an authorization flaw that allows authenticated users to access the complete device shadow of any device by specifying its device ID. This vulnerability exposes sensitive information, such as device credentials, owner details, network data, and telemetry, without verifying any relationship between the requester and the target device.

CISA Malcolm

Summary

The following versions of **CISA Malcolm** are affected:

- **Malcolm**
- **CVSS v3 8.8**
- **Vendor:** CISA
- **Equipment:** CISA Malcolm
- **Vulnerabilities:** Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Limitation of a Pathname to a

Restricted Directory ('Path Traversal'), Server-Side Request Forgery (SSRF), Authentication Bypass by Spoofing, Missing Authorization, Missing Authentication for Critical Function, Incorrect Authorization, Use of Default Credentials, Improper Certificate Validation, URL Redirection to Untrusted Site ('Open Redirect'), Dependency on Vulnerable Third-Party Component, Use of Password Hash With Insufficient Computational Effort

Vulnerabilities

CVE ID	Base Severity	Description
CVE-2026-90443	Medium	A web interface reflects a portion of the request URL into a script context and a hyperlink attribute without adequate encoding, and does not require authentication to reach. This allows an unauthenticated network attacker to craft a link that, when visited by a user, executes arbitrary script in the context of the affected application and can redirect the user's browser to an arbitrary external site. Successful exploitation could allow an attacker to act with the compromised user's session privileges within the application.
CVE-2026-90444	High	A file-transfer interface that requires valid credentials accepts attacker-controlled filenames without restricting shell metacharacters. An automated process later constructs and runs a system command using the uploaded file's name, allowing an authenticated attacker to embed and execute arbitrary operating system commands with the privileges of that process. This allows an attacker to read and modify ingested log data, and could provide a foothold for further movement within the internal network.
CVE-2026-90445	High	An interface that accepts file uploads from authenticated users extracts the contents of uploaded archives without validating that extracted file paths remain within the intended destination directory. This allows an authenticated attacker to craft an archive whose entries traverse outside the destination directory, causing the extraction process to write files to arbitrary locations with the privileges of that process. This could allow an attacker to inject fabricated records into the system's stored data or tamper with application configuration.
CVE-2026-90446	Medium	An application programming interface endpoint accepts a user-supplied value and interpolates it directly into the path of a backend request to the underlying search and analytics data store, without restricting its contents. This allows an authenticated attacker to substitute an arbitrary backend path, causing the application's own elevated service credentials to be used against unintended internal endpoints. This could allow an attacker to enumerate or read internal configuration and administrative data from the backend data store that would otherwise be restricted.
CVE-2026-90447	High	A routing rule selects between two different authentication mechanisms for the same downstream service based on the value of a client-supplied request header, rather than on any property the client cannot control. An authenticated user in possession of a shared service credential can set this header to route around the primary role-based authorization check and reach the alternate path's fixed, elevated role instead. This allows a low-privileged authenticated attacker who knows the shared credential to perform actions reserved for a higher-privileged role.
CVE-2026-90448	High	A deployment mode intended to expose only read access to stored

		data proxies a set of application programming interface routes without restricting which request methods are allowed. One such route accepts a request that creates or overwrites a stored record, including an attacker-chosen identifier, using the application's own elevated backend credentials. This allows an authenticated user on a deployment intended to be read-only to forge or overwrite stored records that should not be modifiable in that deployment mode.
CVE-2026-90449	Medium	When a particular authentication mode is configured, the reverse proxy forwards requests for a bundled third-party administrative interface directly to that interface without applying the gateway's own authentication requirement first. All access control for this administrative interface, which manages the credential store used to gate every other service in the deployment, is delegated entirely to that third-party interface's own login mechanism. Any authentication weakness in that bundled interface would compromise the credential store protecting the rest of the deployment.
CVE-2026-90450	Medium	The application's role-authorization lookup defaults to granting access when a request handler's name is not present in its table of role requirements, rather than defaulting to deny. Any request handler that is not explicitly registered in this table is reachable by any authenticated user regardless of their assigned role, and any newly added handler is fail-open by default until explicitly added to the table.
CVE-2026-90451	High	An example environment-configuration file ships with a fixed, publicly-known secret value used to sign authentication cookies for a bundled packet-analysis component. A deployment that copies this example file into active configuration without running the setup routine that regenerates the value will use the known default, allowing an attacker aware of the default to forge valid authentication cookies for that component.
CVE-2026-90452	Medium	Requests from the reverse proxy to the identity-provider service for token discovery, introspection, and credential exchange do not verify the identity provider's server certificate. An attacker positioned on the network path between the proxy and the identity provider could impersonate the identity provider and issue forged authentication tokens accepted by the deployment.
CVE-2026-90453	Medium	A file-upload handler redirects the authenticated client's browser to a URL taken directly from that same request's Referer header, without validating it against the application's own origin. This allows an authenticated attacker to craft a request that causes another user's browser to be redirected to an arbitrary external destination after completing an upload.
CVE-2026-90454	Medium	A deployment mode intended to expose only read access to a bundled packet-analysis component's interface denies a list of write-capable routes by pattern, but the pattern omits routes that modify tags attached to stored session records, and the proxy configuration otherwise permits the request method those routes use. This allows an authenticated user on a deployment intended to be read-only to add or remove tags on stored session records.
CVE-2026-90455	Medium	A prior update that raised a bundled HTTP client library to a version remediating known vulnerabilities was later reverted, reintroducing the earlier, vulnerable version into a log-processing component. The only code path in that component using the library issues a request to a single fixed, trusted vendor URL at initialization and does not process attacker-controlled input

		through the library, limiting practical exploitability of the reintroduced version in this context
CVE-2026-90456	Critical	An example environment-configuration file for a bundled inventory-management component ships with a fixed, publicly-known administrative password. A deployment that copies this example file into active configuration without running the setup routine that regenerates credentials will expose that component's administrative interface to anyone aware of the default value.
CVE-2026-90457	Medium	The administrative password is hashed using a comparatively weak, fast algorithm for the credential store backing one authentication path, and the file containing that hash is written with permissions allowing it to be read by any local user. This is inconsistent with a separate, stronger hashing algorithm used for the same password on another authentication path. A party able to read this file, including a local user or a party with access to a configuration backup, could feasibly recover the underlying password through offline computation, compromising the administrative credential across every path that accepts it.

Remediations:

- The latest version of Malcolm (September 2026 or later) fixes these vulnerabilities. Affected users are encouraged to update their instance of Malcolm to the latest version.

References:

<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-01>
<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-02>
<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-03>
<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-04>
<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-05>
<https://www.cisa.gov/news-events/ics-advisories/icsa-26-274-06>
<https://www.cisa.gov/news-events/ics-advisories/icsa-26-254-01>

CVEs

CVE-2023-46604,	CVE-2026-15953,	CVE-2026-90448,
CVE-2026-94591,	CVE-2026-64892,	CVE-2026-90449,
CVE-2026-94592,	CVE-2026-64893,	CVE-2026-90450,
CVE-2026-94593,	CVE-2026-101104,	CVE-2026-90451,
CVE-2026-94594,	CVE-2026-96613,	CVE-2026-90452,
CVE-2023-95102,	CVE-2026-90443,	CVE-2026-90453,
CVE-2026-97363,	CVE-2026-90444,	CVE-2026-90454,
CVE-2026-97212,	CVE-2026-90445,	CVE-2026-90455,
CVE-2026-93474,	CVE-2026-90446,	CVE-2026-90456,
CVE-2026-15952,	CVE-2026-90447,	CVE-2026-90457

