DOCUMENT ID: 9AKK108470A8565
REVISION: A
RELEASE DATE: 11 MARCH 2025

ABB MEASUREMENT & ANALYTICS | CYBER SECURITY ADVISORY

Vulnerability in the Web UI (REST Interface)

RMC-100

CVE ID: CVE-2022-24999

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, expressed or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

Purpose

ABB has a rigorous internal cyber security continuous improvement process which involves regular testing with industry leading tools and periodic assessments to identify potential product issues. Occasionally an issue is determined to be a design or coding flaw with implications that may impact product cyber security.

When a potential product vulnerability is identified or reported, ABB immediately initiates our vulnerability handling process. This entails validating if the issue is in fact a product issue, identifying root causes, determining what related products may be impacted, developing a remediation, and notifying end users and governmental organizations.

The resulting Cyber Security Advisory intends to notify customers of the vulnerability and provide details on which products are impacted, how to mitigate the vulnerability or explain workarounds that minimize the potential risk as much as possible. The release of a Cyber Security Advisory should not be misconstrued as an affirmation or indication of an active threat or ongoing campaign targeting the products mentioned here. If ABB is aware of any specific threats, it will be clearly mentioned in the communication.

The publication of this Cyber Security Advisory is an example of ABB's commitment to the user community in support of this critical topic. Responsible disclosure is an important element in the chain of trust we work to maintain with our many customers. The release of an Advisory provides timely information which is essential to help ensure our customers are fully informed.

Affected products

After investigating, it is determined that the RMC-100 with REST interface is affected. The vulnerability is only present when the REST interface is enabled. This interface is disabled by default.

Table 1 : Affected products

Product	Software version
RMC-100	2105457-036 to 2105457-044 inclusive
RMC-100 LITE	2106229-010 to 2106229-016 inclusive

Vulnerability ID

Table 2: Vulnerability ID

CVE ID	Name
CVE-2022-24999	QS Querystring

Summary

An update is available that resolves a vulnerability in the product versions listed in Table 1.

An attacker who successfully exploited this vulnerability could cause the web UI to stop.

Recommended immediate actions

The problem is corrected in the following product versions:

- RMC-100 Customer Package (2105452-048)
- RMC-100 LITE Customer Package (2106260-017)

ABB recommends that customers apply the update at their earliest convenience. Please find these updates here: RMC - Flow Computers (Flow Computers, Remote Controllers and RTUs) | Flow Computers | ABB.

Vulnerability severity and details

A vulnerability exists in the web UI (REST interface) included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the web UI node, causing a Node process hang and requiring restart of the REST interface (disable/enable).

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both v3.1 and v4.0.

Table 3: CVE-2022-24999 details

Item	Description
CVSS v3.1 Base Score	7.5 HIGH
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
NVD Summary Link	https://nvd.nist.gov/vuln/detail/cve-2022-24999
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Proto-type Pollution')

NOTE: For the CVSS v3.1 scoring, only the CVSS Base Score and the Temporal Score (if information is available) are considered in this advisory. The CVSS Environmental Score, which can affect the vulnerability severity, is not provided in this advisory since it reflects the potential impact of a vulnerability within the end-user organizations' computing environment; end-user organizations are therefore recommended to analyze their situation and specify the Environmental Score.

For the CVSS v4.0 scoring, only the CVSS Base Metrics and the CVSS Supplemental Metrics (if information is available) are considered in this advisory. The CVSS Environmental and Threat Metrics, which can affect the vulnerability severity, are not provided in this advisory since they reflect the potential impact of a vulnerability within the end-user organizations' computing environment and over time depending on the vulnerability exploit maturity. Therefore, end-user organizations are recommended to analyze their situation and specify the Environmental and Threat Metrics.

Mitigating factors

ABB recommends disabling the REST interface when not in use to configure the MQTT functionality. By default, the REST interface is disabled so no risk is present.

The RMC-100 is not intended for access over public networks such as the internet. An attacker would need to have access to the customer's private control network to exploit this vulnerability. Proper network segmentation is recommended. See General security recommendations, for further advice on how to keep your system secure.

Workarounds

The vulnerability is only present when the REST interface is enabled. Only enable the REST interface when needed for the configuration of MQTT. Ensure that the REST interface is disabled after finishing configuring MQTT utilities.

Frequently asked questions

What causes the vulnerability?

The vulnerability is caused by a vulnerability in the component QS Querystring that is used in the web UI.

What is the affected product or component?

The RMC-100 web UI.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the web UI to become unresponsive until the REST interface is disabled and enabled.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by creating a specially crafted message and sending the message to an affected web UI node. This would require that the attacker has access to the system network by connecting to the network either directly or through a wrongly configured or penetrated firewall. Or the attacker installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks. See Mitigating factors.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include: process control systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.

What does the update do?

The update removes the vulnerability by modifying the way that the web UI processes the URL.

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, a notification about this vulnerability was issued in 2024 and measures to resolve the issue were started immediately.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited when this security advisory was originally issued.

General security recommendations

For any installation of software-related ABB products, we strongly recommend the following (non-exhaustive) list of cyber security practices:

- Isolate special-purpose networks (e.g., for automation systems) and remote devices behind firewalls and separate them from any general-purpose network (e.g., office or home networks).
- Install physical controls so no unauthorized personnel can access your devices, components, peripheral equipment, and networks.
- Never connect programming software or computers containing programming software to any network other than the network for the devices that it is intended for.
- Scan all data imported into your environment before use to detect potential malware infections.
- Minimize network exposure for all applications and endpoints to ensure that they are not accessible from the Internet unless they are designed for such exposure and the intended use requires such.
- Ensure all nodes are always up to date in terms of installed software, operating system, and firmware patches as well as anti-virus and firewall.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

Support

For additional instructions and support, please contact your local ABB service organization. For contact information, see https://new.abb.com/contact-centers.

Information about ABB's cyber security program and capabilities can be found at http://www.abb.com/cybersecurity.

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	2-12-2025