DOCUMENT ID: 9AKK108471A3623
REVISION: A
DATE: 2025-07-03

CYBER SECURITY ADVISORY

Vulnerabilities in web UI (REST Interface)

RMC-100

CVE-2025-6074: Authentication Bypass to the MQTT configuration Web Interface

CVE-2025-6073: Stack Buffer Overflow in MQTTCore

CVE-2025-6072: Stack Buffer Overflow in MQTTCore

CVE-2025-6071: Hard Coded Key used for AES encryption

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.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

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 vulnerabilities are only present when the REST interface is enabled. This interface is disabled by default.

Product	Software version
RMC-100	2105457-043 to 2105457-045 inclusive
RMC-100 LITE	2106229-015 to 2106229-016 inclusive

Vulnerability IDs

CVE ID	Title
CVE-2025-6074	Authentication Bypass to the MQTT configuration Web Interface
CVE-2025-6073	Stack Buffer Overflow in MQTTCore
CVE-2025-6072	Stack Buffer Overflow in MQTTCore
CVE-2025-6071	Hard Coded Key used for AES encryption

Summary

ABB is aware of vulnerabilities in the product versions listed above.

An attacker who successfully exploited these vulnerabilities could gain unauthenticated access to the MQTT configuration data (CVE-2025-6074), cause a DoS on the MQTT configuration web server (REST interface) (CVE-2025-6073, CVE-2025-6072), or decrypt encrypted MQTT broker credentials (CVE-2025-6071).

Recommended immediate actions

ABB is currently investigating the vulnerabilities to provide adequate protection to customers.

ABB recommends that customers apply the recommended mitigations.

Vulnerability severity and details

Vulnerabilities exist in the web UI (REST Interface) included in the product versions listed above. An attacker could exploit the vulnerabilities by sending specially crafted messages to the system node, causing the node to stop, manipulate MQTT configuration, or decrypt MQTT information.

CVE ID	Details
CVE-2025-6074	CWE-321: Use of Hard-coded Cryptographic Key When the REST interface is enabled by the user, and an attacker gains access to source code and control network, the attacker can bypass the REST interface authentication and gain access to MQTT configuration data.
CVE-2025-6073	CWE-121 : Stack-based Buffer Overflow When the REST interface is enabled by the user, and an attacker gains access to the control network, and user/password broker authentication is enabled, and CVE-2025-6074 is exploited, the attacker can overflow the buffer for username or password.
CVE-2025-6072	CWE-121 : Stack-based Buffer Overflow When the REST interface is enabled by the user, and an attacker gains access to the control network, and CVE-2025-6074 is exploited, the attacker can use the JSON configuration to overflow the date of expiration field.
CVE-2025-6071	CWE-321: Use of Hard-coded Cryptographic Key An attacker can gain access to salted information to decrypt MQTT information.

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

[1] 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.

CVE ID	Details	
CVE-2025-6074	CVSS v4.0 Base Score:	6.3 / Medium
	CVSS v4.0 Vector:	AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N
	NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2025-6074
	CVSS v3.1 Base Score:	6.5 / Medium
	CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVE-2025-6073	CVSS v4.0 Base Score:	8.2 / High
	CVSS v4.0 Vector:	AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
	NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2025-6073
	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
CVE-2025-6072	CVSS v4.0 Base Score:	8.2 / High
	CVSS v4.0 Vector:	AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
	NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2025-6072
	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
CVE-2025-6071	CVSS v4.0 Base Score:	6.3 / Medium
	CVSS v4.0 Vector:	AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N
	NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2025-6071
	CVSS v3.1 Base Score:	5.3 / Medium
	CVSS v3.1 Vector:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Mitigating factors

ABB recommends disabling the REST interface when not being used 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.

Frequently asked questions

What causes the vulnerability?

The vulnerabilities are caused by hard-coded keys, and unchecked buffers in the web UI (REST interface).

What is the affected product or component?

The RMC-100 and Lite web UI that is used to configure the MQTT protocol are affected.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause the affected system node to stop or become inaccessible.

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 system node. This would require the attacker to have access to the system network, either directly or through an incorrectly configured or penetrated firewall.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability.

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

No, ABB received information about this vulnerability through responsible disclosure.

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 programing 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.

Acknowledgement

ABB thanks Claroty Team82 Research for helping to identify the vulnerabilities and protecting our customers.

Support

For additional instructions and support, please contact your local ABB service organization. For contact information, see www.abb.com/contactcenters.

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

Revision history

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
A	all	Initial version	3 July 2025