DOCUMENT ID: 4TZ00000006008
REVISION: A
DATE: 2025-10-08

CYBER SECURITY ADVISORY

LVS MConfig
Insecure memory handling

CVE ID: CVE-2025-9970

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, express 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

Product	version
MConfig	V1.4.9.21 and older

Vulnerability IDs

CVE ID: CVE-2025-9970

Summary

ABB became aware of an internally discovered vulnerability in the **MConfig** product listed above.

An attacker with access to local networks who successfully exploits vulnerability could have access to application's sensitive information.

ABB strongly advises customers to update **MConfig** with latest software version.

Recommended immediate actions

The vulnerability is resolved in the following product versions:

MConfig version 1.4.9.22

ABB advises users to update their devices to the latest software version.

Additionally, ABB recommends implementing defensive measures to reduce the risk of vulnerability exploitation, as outlined in the product instruction manual. Please refer to the section “Mitigation factors” for more information.

Vulnerability severity and details

ABB has become aware of the following vulnerability.

The severity assessment has been performed by using the FIRST Common Vulnerability Scoring System (CVSS) for both v3.1[1] and v4.0[2].

The indicated Common Weakness Enumerations (CWE) have been selected from the MITRE CWE list[3].

CVE ID	Title	
CVE-2025-9970	**Application credential stored in clear text in memory.**	
Description	During the runtime of the MConfig Software application, an attacker can export the memory dump file into the operating system. If passwords are stored in plain text in memory, they will be included in these dump files. If such dump files are mishandled, attackers could obtain them and extract the passwords.	
CWE	CWE-316: Cleartext Storage of Sensitive Information in Memory.	
CVSS v3.1	Base Score:	7.4
	Temporal Score:	6.7
	Vector:	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:H/A:H/E:P/RL:O
CVSS v4.0	Score:	5.7
	Vector:	CVSS:4.0/AV:L/AC:H/AT:P/PR:L/UI:P/VC:L/VI:H/VA:H/SC:N/SI:N/SA:H
CVE NVD Summary Link	https://nvd.nist.gov/vuln/detail/CVE-2025-9970	

[1] 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.

[2] 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.

[3] Common Weakness Enumeration (CWE), The MITRE Corporation, https://cwe.mitre.org/.

Mitigating factors

Mitigating factors describe conditions and circumstances that make an attack that exploits the vulnerability difficult or less likely to succeed.

In case customer cannot upgrade the firmware or it is not feasible then please immediately apply mitigating factors mentioned in "General security recommendations".

Frequently asked questions

What causes the vulnerability?

The vulnerability is caused by code defect allowing the attacker to extract the sensitive information such as user credentials from memory dump of the application. Please refer to ***Vulnerability severity and details*** for further details.

What is MConfig ?

MConfig is the parameterizing software for ABB LV switchgear components such as motor and feeder controller, operation panel, temperature monitoring solutions and protocol converter. The components are physically installed in a low voltage switchgear located in switch rooms that require authority to access.

To run this software on a host machine (computer), the operating system should be Win11 or later version.

What might an attacker use the vulnerability to do?

If the mentioned vulnerability has been successfully exploited by an attacker, this could allow the attacker to extract sensitive information such as user credentials.

With user credentials and access to a host machine with MConfig installed, and access to the switch room with components installed in a switchgear, the attacker can modify the setting of the components potentially compromising its correct operation.

How could an attacker exploit vulnerability?

An attacker with host machine physical access could, after a user log into MConfig, exploit a vulnerability by exporting a memory dump during runtime, potentially exposing the user's password.

Could vulnerability be exploited remotely?

The vulnerability can only be exploited if an attacker has physical access to the host machine with MConfig software.

What does the update do?

MConfig version V1.4.9.22 update has fix for the vulnerability mentioned in ***Vulnerability severity and details*** section.

The measures below were implemented to fix the vulnerability:

- Clear any authentication-related memory data after a successful login.
- Hash the passwords in SHA256.

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

No, the vulnerability mentioned has not been publicly disclosed.

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 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	08-Oct-2025