DOCUMENT ID: 9AKK108473A3188
REVISION: D
DATE: 2026-09-29

CYBER SECURITY ADVISORY

Mint Workbench I Path traversal Vulnerability

CVE ID：CVE-2026-19438

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.

© Copyright 2026 ABB. All rights reserved.

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

Mint Workbench I 5876 and the versions before

Vulnerability IDs

CVE-2026-19438

Summary

A local attacker who successfully exploited this vulnerability could gain elevated privileges by Path Traversal, arbitrarily reading files of system, to cause confidentiality impact of system files.

Recommended immediate actions

Mint Workbench I 5876 and the versions before, are impacted, customers who use these products, should:

- Disable Service MWI http when it is not in active use.
- Restrict physical machine access to authorized personnel only.
- Avoid storing sensitive or confidential data on any hosts running service MWI http.
- Enable User Account Control (UAC) to block unauthorized privilege escalation attempts.

These actions above are the only measures available. No further patch will be released because this product reaches end-of-life globally (out of China) by the end of 2026 and in China by the end of 2027.

© Copyright 2026 ABB. All rights reserved.

Vulnerability severity and details

A vulnerability exists in the Mint Workbench I, the versions listed above. A local attacker who successfully exploited this vulnerability could gain elevated privileges by Path Traversal, arbitrarily reading files of system, to cause confidentiality impact of system files.

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

CVE-2026-19438 Mint Workbench I Path traversal Vulnerability

CVSS v3.1 Basic score: 7.5 (High)

CVSS v3.1 Temporal score: 7.5 (High)

CVSS v3.1 Vector: https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 score: 8.2 (High)

CVSS v4.0 Vector: https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2026-19438

Mitigating factors

To exploit the vulnerability the attacker needs to have local access to the machine beforehand and have file write access in the path.

Please also refer to section “General security recommendations” for further advise on how to keep your system secure.

Workarounds

Mint Workbench I 5876 and the versions before, are impacted. Customers who use these products should:

- Disable Service MWI http when it is not in active use.

[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.

© Copyright 2026 ABB. All rights reserved.

- Restrict physical machine access to authorized personnel only.
- Avoid storing sensitive or confidential data on any hosts running service MWI http.
- Enable User Account Control (UAC) to block unauthorized privilege escalation attempts.

Frequently asked questions

What causes the vulnerability?

The vulnerability is caused by a local attacker gaining elevated privileges through Path Traversal of http server in the Mint Workbench I.

What is Mint Workbench I?

Mint Workbench I is a comprehensive Windows GUI for MINT programming and provides a user-friendly interface for commissioning Micro Flex and Moti Flex servo drives, to guide users to complete servo and motor configuration and commission. Mint Workbench I is also embedded to ABB Automation Builder.

What might an attacker use the vulnerability to do?

A local attacker could acquire privileges to cause confidentiality impact of system files by arbitrarily reading files of system.

How could an attacker exploit the vulnerability?

An attacker could try to exploit vulnerability by http Path Traversal. This would require that the attacker has access to the system locally. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

No, to exploit this vulnerability an attacker would need to be locally logged into an affected system node.

Can functional safety be affected by an exploit of this vulnerability?

Functional safety is not affected by this vulnerability.

What does the update do?

There are no updates
This product has very few remaining users and is scheduled for discontinuation by end of 2026 internationally (out of China), and discontinuation by end of 2027 in China.

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.

© Copyright 2026 ABB. All rights reserved.

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 thank Sandeep Vatada for working with ABB in effort to protect 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	17.9.2026
B		Update link, add missing info, etc.	20.9.2026
C		Reviewed	22.9.2026
D		MWI introduction	29.9.2026

© Copyright 2026 ABB. All rights reserved.