DOCUMENT ID: 9AKK108469A7912
REVISION: A
DATE: 2024-07-05

CYBER SECURITY ADVISORY

Mint Workbench I Unquoted Service Path Enumeration

CVE ID: CVE-2024-5402

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.

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 through version 5866

Vulnerability IDs

CVE-2024-5402

Summary

An update is available that resolves a vulnerability in the product versions listed above. We found this during internal testing and the vulnerability has been fixed since 2021 in version 5868, but it has come to our attention that some customers might still be using old vulnerable versions.

A local attacker who successfully exploited this vulnerability could gain elevated privileges by inserting an executable file in the path of the affected service.

Recommended Immediate Actions

This vulnerability is resolved since Mint Workbench I version 5868 which is released in 2021.

ABB recommends customers to verify the version installed with checking version information either shows on startup page or" help-about mint workbench" menu.

In case of still be using old vulnerable version please apply the update at earliest convenience, download the S/W from official ABB website , click installation executable for a full upgrade, version information

can be identified on initial page. click next button on each step, old version that is installed will be auto detected and removed in the installation process.

Vulnerability severity and details

A vulnerability exists in the Mint Workbench I included in the product versions listed above. A local attacker who successfully exploited this vulnerability could gain elevated privileges by inserting an executable file in the path of the affected service.

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

CVE-2024-5402 - Mint Workbench I Unquoted Service Path Enumeration

A local attacker who successfully exploited this vulnerability could gain elevated privileges by inserting an executable file in the path of the affected service.

CVSS v3.1 Base Score: 7.8
CVSS v3.1 Temporal Score: 7.0
CVSS v3.1 Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

CVSS v4.0 Score 6.2
CVSS v4.0 Vector:
CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:L/SC:L/SI:H/SA:H/S:N/AU:Y/R:U/V:C/RE:L/U:Clear

NVD Summary Link: https://nvd.nist.gov/vuln/detail/CVE-2024-5402

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

1. Start the registry editor (administrator privileges are needed).

2. Open the registry entry Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Mint HTTP Server.

3. Enclose the string value that is entered under "ImagePath" with quotation marks. Example: "C:\Program Files (x86)\ABB\Mint WorkBench\Mint HTTP Server\MintHTTPServer.exe".

[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.

Frequently asked questions

What causes the vulnerability?

The vulnerability is caused by common weakness Unquoted Search Path or Element (CWE-428) in implementation. Product use path that contains an unquoted element, in which the element contains whitespace or other separators, if a malicious individual has access to the file system, it is possible to elevate privileges by inserting executable to be run by a privileged program.

What is Mint Workbench I?

Mint Workbench I is a comprehensive Windows GUI for MINT programming and provides a user-friendly interface for commissioning MicroFlex and MotiFlex servo drives, to guide users to complete servo and motor configuration and commission.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could causes a local attacker gaining elevated privileges on the affected system through inserting an executable file in the path of the mint server in the Mint Workbench I.

How could an attacker exploit the vulnerability?

An attacker could try to exploit the vulnerability by inserting an executable file in the path of the mint server. 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 have physical access to 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?

The update removes the vulnerability by adding a quote at the start and end of the path to enclose the path of Mint server.

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 Yoav Yehudai of Novartis 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	2024-07-05