DOCUMENT ID: 9AKK108467A0305
REVISION: B
DATE: 2022-08-23

CYBER SECURITY ADVISORY

Link Following Local Privilege Escalation Vulnerabilities in ABB Automation Builder, Drive Composer and Mint WorkBench
ABBVREP0072
CVE-2022-31216
CVE-2022-31217
CVE-2022-31218
CVE-2022-31219
CVE-2022-26057

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

Drive Compose entry versions 2.0 – 2.7

Drive Composer pro versions 2.0 – 2.7

ABB Automation Builder 1.1.0 – 2.5.0

Mint WorkBench build 5866 and older

Vulnerability IDs

IDs	Name
ABBVREP0072	Link Following Local Privilege Escalation Vulnerabilities in ABB Automation Builder, Drive Composer and Mint WorkBench
CVE-2022-31216	Drive Composer Link Following Local Privilege Escalation Vulnerability
CVE-2022-31217	Drive Composer Link Following Local Privilege Escalation Vulnerability
CVE-2022-31218	Drive Composer Link Following Local Privilege Escalation Vulnerability
CVE-2022-31219	Drive Composer Link Following Local Privilege Escalation Vulnerability
CVE-2022-26057	Mint WorkBench Link Following Local Privilege Escalation Vulnerability

Summary

Updates are available that resolve publicly reported vulnerabilities in the product versions listed above.

An attacker who successfully exploited this vulnerability could insert and run arbitrary code on the system.

Recommended immediate actions

The problem is corrected in the following product versions:

- ABB Automation Builder 2.5.1 (link to download page)
- Drive Composer entry version 2.7.1 (link to download page)
- Drive Composer pro version 2.7.1 (link to download page)
- Mint WorkBench Build 5868 (link to download page)

ABB recommends that customers apply the update at earliest convenience. Updated versions of ABB Automation Builder, Drive Composer and Mint WorkBench are available.

Vulnerability severity and details

Vulnerabilities exist in the Drive Composer installer included in the product versions listed above. An attacker could exploit the vulnerability by inserting and run arbitrary code. This requires that some of the files in Drive Composer installer are replaced with malicious files prior to installing the application or using the repair function of the installer.

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

CVE-2022-31216 Drive Composer Link Following Local Privilege Escalation Vulnerability

Vulnerabilities in the Drive Composer allow a low privileged attacker to create and write to a file anywhere on the file system as SYSTEM with arbitrary content as long as the file does not already exist.

The Drive Composer installer file allows a low-privileged user to run a "repair" operation on the product.

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	7.0
CVSS v3.1 Vector:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:R/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H&version=3.1

[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-2022-31217 Drive Composer Link Following Local Privilege Escalation Vulnerability

Vulnerabilities in the Drive Composer allow a low privileged attacker to create and write to a file anywhere on the file system as SYSTEM with arbitrary content as long as the file does not already exist.

The Drive Composer installer file allows a low-privileged user to run a "repair" operation on the product.

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	7.0
CVSS v3.1 Vector:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:R/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H&version=3.1

CVE-2022-31218 Drive Composer Link Following Local Privilege Escalation Vulnerability

Vulnerabilities in the Drive Composer allow a low privileged attacker to create and write to a file anywhere on the file system as SYSTEM with arbitrary content as long as the file does not already exist.

The Drive Composer installer file allows a low-privileged user to run a "repair" operation on the product.

CVSS v3.1 Base Score:	7.8
CVSS v3.1 Temporal Score:	7.0
CVSS v3.1 Vector:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:R/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H&version=3.1

CVE-2022-31219 Drive Composer Link Following Local Privilege Escalation Vulnerability

Vulnerabilities in the Drive Composer allow a low privileged attacker to create and write to a file anywhere on the file system as SYSTEM with arbitrary content as long as the file does not already exist.

The Drive Composer installer file allows a low-privileged user to run a "repair" operation on the product.

CVSS v3.1 Base Score:	7.3
CVSS v3.1 Temporal Score:	6.5
CVSS v3.1 Vector:	AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:F/RL:O/RC:R/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:L/MUI:N/MS:U/MC:H/MI:H/MA:H&version=3.1

CVE-2022-26057 Mint WorkBench Link Following Local Privilege Escalation Vulnerability

Vulnerabilities in the Mint WorkBench allow a low privileged attacker to create and write to a file anywhere on the file system as SYSTEM with arbitrary content as long as the file does not already exist.

The Mint WorkBench installer file allows a low-privileged user to run a "repair" operation on the product.

CVSS v3.1 Base Score:	6.7
CVSS v3.1 Temporal Score:	6.0
CVSS v3.1 Vector:	AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

NVD Summary Link:	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:R/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:H/MUI:N/MS:U/MC:H/MI:H/MA:H&version=3.1

Workarounds

ABB has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they can help block known attack vectors. When a workaround reduces functionality, this is identified below as “Impact of workaround”.

With ABB Automation Builder it is possible to change the version of Drive Composer used so it is not mandatory to update that application immediately. Steps:

1) Install or upgrade Drive Composer pro version to 2.7.1
2) In ABB Automation Builder Options, select External tools.
3) At Drive composer pro-line, select Custom and select the installed Drive Composer pro version 2.7.1 executable typically in C:\Program Files (x86)\DriveWare\Drive Composer pro\2.7

Alternatively, users are able to remove the vulnerable Drive Composer for ABB Automation Builder. This can be done either from ABB Automation Builder Installation manager or from Windows Settings: Apps & features.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploited this vulnerability could take control of an affected system node or insert and run arbitrary code in an affected system node.

What causes the vulnerability?

The vulnerability is caused by the Drive Composer and Mint WorkBench installer repair functions granting unnecessary permissions for the application in the installation folder. It is possible for an attacker to make the installer install unwanted files to the system by replacing some of the files in the installer.

What is Drive Composer?

Drive Composer is a start-up and maintenance tool for ABB's common architecture drives. The tool is used to view and set drive parameters, and to monitor and tune process performance.

The entry version of Drive Composer provides basic functionality for setting parameters, basic monitoring, taking local control of the drive from the PC, and event logger handling. Drive Composer pro is the full-fledged commissioning and troubleshooting tool. Drive Composer pro is also embedded to ABB Automation Builder.

What is ABB Automation Builder?

ABB Automation Builder is the integrated software suite for machine builders and system integrators wanting to automate their machines and systems in a productive way. ABB Automation Builder covers the engineering of AC500 PLCs, AC500 safety PLCs, CP600 control panels, drives and motion.

What is MintWorkBench?

Mint Workbench is a software tool designed for commissioning MotiFlex e180, MicroFlex e190 servo drives and eSM, HDS series servo motors.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could allow the attacker to take control of the system node.

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 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 that he installs malicious software on a system node or otherwise infects the network with malicious software. 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 local access to an affected system node.

What does the update do?

The update removes the vulnerability by modifying the way that the Drive Composer and Mint Work-Bench installers handle the permissions of the filesystem.

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.

More information on recommended practices can be found in the following documents:

3AXD10000492137	Technical guide - Cybersecurity for ABB drives
3ADR010317	White Paper - AC500 Cyber Security

Acknowledgement

This vulnerability was discovered by Michael DePlante (@izobashi) of Trend Micro Zero Day Initiative. ABB appreciates their actions to keep our products safe for our customers.

References

Following advisories are the original reported advisories reported to this document:

ZDI-CAN-16276 ABB Automation Builder Platform Link Following Local Privilege Escalation Vulnerability

ZDI-CAN-16277 ABB Automation Builder Platform Link Following Local Privilege Escalation Vulnerability

ZDI-CAN-16281 ABB Automation Builder Platform Link Following Local Privilege Escalation Vulnerability

ZDI-CAN-16321 ABB Automation Builder Platform Link Following Local Privilege Escalation Vulnerability

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	2022-06-13
B	p 3	Updated information about availability of fixes (“Recommended immediate actions”)	2022-08-23