DOCUMENT ID: 9AKK108470A5466
REVISION: C
DATE: 2025-02-05

CYBER SECURITY ADVISORY

Drive Composer Path Traversal Vulnerability

CVE ID: CVE-2024-48510

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

Drive Composer entry version 2.9.0.1 and earlier.

Drive Composer pro version 2.9.0.1 and earlier.

Vulnerability ID

CVE-2024-48510

Summary

An update is available that resolves vulnerability in the product versions listed above.

An attacker who successfully exploits the vulnerability could get unauthorized access to the file system on the host machine. This can lead to the execution of arbitrary code, data leakage, or even complete system compromise.

Recommended immediate actions

The vulnerability mentioned in this advisory has been corrected in Drive Composer version 2.9.1.

Drive Composer version 2.9.1 (both entry and pro) is downloadable from the product page:
https://new.abb.com/drives/software-tools/drive-composer

ABB recommends that customers apply the update at earliest convenience.

Vulnerability severity and details

A vulnerability exists in the Drive Composer in the product versions listed above. Directory Traversal vulnerability in DotNetZip v.1.16.0 and earlier versions allows a remote attacker to extract files to arbitrary locations.

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

CVE-2024-48510, directory traversal vulnerability

Vulnerability in drive composer can allow attackers unauthorized access to the file system on the host machine. An attacker can exploit this flaw to run malicious code, which could lead to the compromise of the affected system.

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	8.4
CVSS v3.1 Vector:	VSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	https://nvd.nist.gov/vuln/detail/CVE-2024-48510

Weakness Enumeration

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

Mitigating factors

The identified vulnerability could be exploited when a user opens a tampered Drive Composer file (such as a support package or parameter backup). Users are advised to only open Drive Composer files received from trusted sources and ensure they are free from any alterations by scanning the files through a malware scanner.

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

Frequently asked questions

What is the scope of this vulnerability?

CVE-2024-58510: Vulnerability in Drive Composer file can allow attackers unauthorized access to the file system on the host machine. An attacker can exploit this flaw to run malicious code, which could lead to the compromise of the affected system.

[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.

What causes this vulnerability?

Mentioned vulnerability is caused by outdated versions of third-party library (DotNetZip 1.6 or earlier).

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 might an attacker use the vulnerability to do?

An attacker who successfully exploits the vulnerability could get unauthorized access to the file system on the host machine. This can lead to the execution of arbitrary code, data leakage, or even complete system compromise.

How could an attacker exploit the vulnerability?

An attacker can create a malicious Drive Composer file (such as a support package or parameter backup), when handled by the vulnerable Drive Composer version, enables them to extract files to arbitrary locations.

Could the vulnerability be exploited remotely?

No.

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

No.

What does the update do?

With Drive Composer 2.9.1 the third-party library affected with known vulnerability have been replaced with library unaffected by this vulnerability.

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

Yes, third-party vulnerability has been publicly disclosed. The impact on Drive Composer has not been previously 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 vulnerability in Drive Composer 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 net-work 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

References

CVE-2024-48510 - Directory Traversal vulnerability in DotNetZip.

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	10-01-2025
B	all	Formatting improvement	21-01-2025
C	all	CVE number typographical error correction	05-02-2025