DOCUMENT ID: 9AKK108467A7957
REVISION: B
DATE: 2023-07-10

CYBER SECURITY ADVISORY

Drive Composer multiple vulnerabilities

CVE ID: CVE-2018-1002205, CVE-2018-1285, CVE-2022-35737, CVE-2021-27293, CVE-2022-37434

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

CVE-2018-1285, CVE-2022-35737, CVE-2021-27293, CVE-2022-37434:

Drive Composer entry 2.8 and earlier

Drive Composer pro 2.8 and earlier.

CVE-2018-1002205:

Drive Composer entry 2.4 and earlier

Drive Composer pro 2.4 and earlier.

Vulnerability IDs

CVE-2018-1002205, CVE-2018-1285, CVE-2022-35737, CVE-2021-27293, CVE-2022-37434

Summary

An update is available that resolves privately reported vulnerabilities in the product versions listed above.

An attacker who successfully exploited these vulnerabilities could cause the product to stop, make the product inaccessible or insert and run arbitrary code.

Recommended immediate actions

All vulnerabilities mentioned in this advisory have been corrected in Drive Composer version 2.8.2.

Drive Composer versions 2.8.2 (both entry and pro) are downloadable from the product page: https://new.abb.com/drives/software-tools/drive-composer

ABB recommends that customers apply the update at earliest convenience.

CVE-2018-1002205 has been fixed already in Drive Composer version 2.5.

CVE-2018-1285, CVE-2021-27293, CVE-2022-37434 have been fixed already in Drive Composer version 2.8.1.

Vulnerability severity and details

A vulnerability exists in the Drive Composer installer included in the product versions listed above. An attacker could exploit the vulnerability by sending a specially crafted message to the system node, causing the node to stop or become inaccessible, allowing the attacker to take control of the product, or insert and run arbitrary code.

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

CVE-2018-1002205, attackers can write to arbitrary files in a Zip archive entry.

Vulnerabilities in Drive Composer file can allow attackers to write to arbitrary files via a ../ (dot dot slash) in a Zip archive entry that is mishandled during extraction.

CVSS v3.1 Base Score:	5.5
CVSS v3.1 Temporal Score:	5.0
CVSS v3.1 Vector:	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
NVD Summary Link:	NVD - CVE-2018-1002208 (nist.gov)

CVE-2018-1285, Apache Log4net Vulnerability

Vulnerabilities in Drive Composer file allows for XXE-based attacks in applications that accept attacker-controlled log4net configuration files as older Apache log4net versions (before 2.0.10) do not disable XML external entities when parsing log4net configuration files.

CVSS v3.1 Base Score:	9.8
CVSS v3.1 Temporal Score:	8.5
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link:	NVD – CVE-2018-1285 (nist.gov)

CVE-2022-35737, SQLite 1.0.12 allows an array-bounds overflow

Vulnerabilities in Drive Composer file allows an array-bounds overflow if billions of bytes are used in a string argument to a C API.

[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.

CVSS v3.1 Base Score: 7.5
CVSS v3.1 Temporal Score: 6.5
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
NVD Summary Link: NVD - CVE-2022-35737 (nist.gov)

CVE-2021-27293, A vulnerable regular expression

A regular expression which is vulnerable to Regular Expression Denial of Service (ReDoS) when converting strings into DateTimes.

CVSS v3.1 Base Score: 7.5
CVSS v3.1 Temporal Score: 6.7
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
NVD Summary Link: NVD - CVE-2021-27293 (nist.gov)

CVE-2022-37434, heap-based buffer over-read and overflow

Vulnerabilities in Drive Composer file has a heap-based buffer over-read or buffer overflow in inflate .c via a large gzip header extra field.

CVSS v3.1 Base Score: 9.8
CVSS v3.1 Temporal Score: 8.5
CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
NVD Summary Link: NVD - CVE-2022-37434 (nist.gov)

Mitigating factors

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

Frequently asked questions

What are the scopes of these vulnerabilities?

CVE-2018-1002205: An attacker who successfully exploits this vulnerability could take control of an affected system node or insert and run arbitrary code in an affected system node.

CVE-2018-1285: An attacker who successfully exploits this vulnerability could affect Drive Composer log files. This allows for XXE-based attacks in applications that accept attacker-controlled log4net configuration files.

CVE-2022-35737: An attacker who successfully exploits SQLite database file may result to crash the application.

CVE-2021-27293: An attacker who successfully exploits this vulnerability could make application non-responsive.

CVE-2022-37434: An attacker who successfully exploits this vulnerability could cause overflow and it could allow memory corruption when deflating. This action will make drive connection non-responsive.

What causes these vulnerabilities?

All mentioned vulnerabilities are caused by outdated versions of third-party libraries.

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 these vulnerabilities could cause the affected system node to stop or become inaccessible, or allow the attacker to take control of the system node, or allow the attacker to insert and run arbitrary code.

For vulnerability **CVE-2022-35737,** an attacker who successfully exploits the vulnerability could cause the affected system node to become non-responsive.

How could an attacker exploit the vulnerabilities?

It is possible to inject malformed data to Drive Composer configuration or data files. An attacker could try to exploit the vulnerabilities allowing Drive Composer to write arbitrary data or files to the system.

Could these vulnerabilities be exploited remotely?

No, to exploit this vulnerability an attacker would need to have local access to an affected system node.

Can functional safety be affected by an exploit of these vulnerabilities?

No

What does the update do?

With Drive Composer pro 2.8.2 the 3rd party libraries affected with known vulnerabilities have been updated to most recent versions.

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

Yes, third-party vulnerabilities have 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 vulnerabilities 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 document:

3AXD10000492137 Technical guide - Cybersecurity for ABB drives

Acknowledgement

ABB appreciates the report from Stuart Paul of Cromarty about CVE-2018-1285 in Drive Composer Pro.

References

CVE-2018-1002205	Zip-Slip vulnerability
CVE-2018-1285	Apache log4net vulnerability
CVE-2022-35737	SQLite vulnerability
CVE-2021-27293	RestSharp vulnerability
CVE-2022-37434	zlib 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	2023/02/10

Rev. Ind.	Page (p) Chapter (c)	Change description	Rev. date
B	Page: 3 Chapter: Recommended immediate actions Page: 5 Chapter: What does the update do?	Updated to reflect the latest version 2.8.2 of Drive Composer (both Entry and pro) where vulnerability CVE-2022-35737 has been resolved. Originally this vulnerability had not been resolved when this advisory was published alongside Drive Composer 2.8.1.	2023/07/10