SEW EURODRIVE

Security Advisory 2024-001

Version: April 15, 2024

Important Information

Security Vulnerability in MOVITOOLS® MotionStudio

Edition 04/2024

31965520/EN

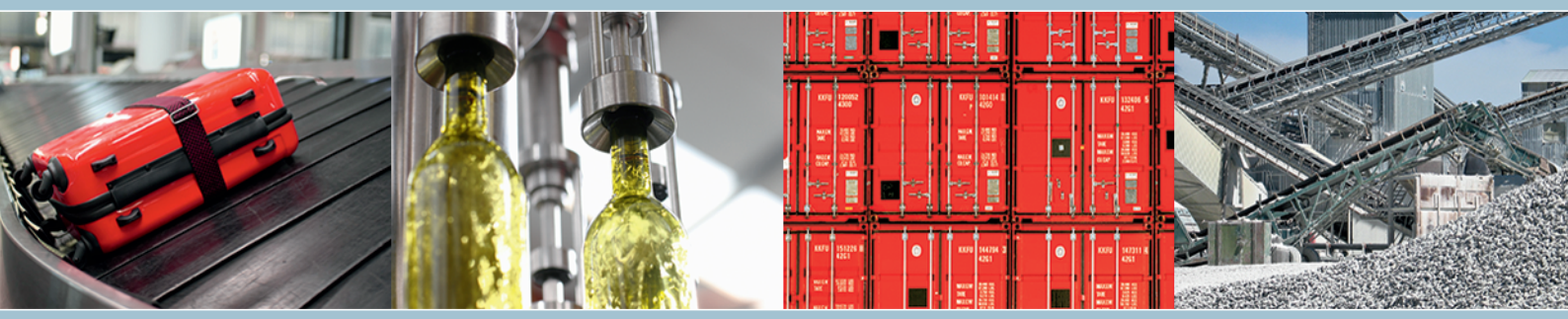


Table of Contents

31965520/EN – 04/2024

1 Security vulnerability in MOVITOOLS® MotionStudio V6.60 or earlier

1.1 Problem

Safety researchers from Trend Micro's Zero Day Initiative have discovered a security vulnerability in MOVITOOLS® MotionStudio. If a specifically prepared project file is opened in the software, it is possible to send data from the local computer to any address.

1.2 Details

While XML files are being processed in the MOVITOOLS® MotionStudio software, unrestricted file access may be possible (CVE-2024-1167). This is due to a security vulnerability that allows XXE injection (CWE-611).

MOVITOOLS® MotionStudio project files are written in XML. This makes it possible for a project file to contain an XML External Entity Reference that allows data to be sent from the engineering PC to any address. This already occurs while the project file is opened. Even if a fault message is displayed, data may still have been sent.

1.3 Affected products

Only MOVITOOLS® MotionStudio version 6.60 or earlier is affected. With of version 6.70 or higher, the problem no longer occurs.

31965520/EN – 04/2024

2 General corrective measures

- Unused active network connections generally increase the security risk. Limit network access to the devices to minimize the risk of attacks.
- Unless absolutely necessary, devices/systems should be disconnected from the higher-level network.
- Prevent unauthorized people or devices from gaining access to affected devices and network segments in which affected devices are being operated.
- If you access the devices with a laptop, use a point-to-point Ethernet connection. The laptops should not be connected to the network.

2.1 Network security and access protection

A bus system can be used to adapt electronic drive components to the system conditions within a wide range. This entails the risk of a parameter change not being visible externally, resulting in unexpected – but not uncontrolled – system behavior, and this may impact negatively on operational safety and reliability, system availability or data security.

Ensure that unauthorized access is prevented, particularly with respect to Ethernet-based networked systems and engineering interfaces.

Use IT-specific safety standards to increase access protection to the ports. For a port overview, refer to the respective technical data of the device in use.

2.2 Access protection and user management

SEW-EURODRIVE recommends that you generally reduce the group of people who can execute engineering tools and transfer potentially harmful files by means of the user management of the system.

31965520/EN – 04/2024

3 Product-specific information and measures

3.1 Immediate measure

Create a firewall rule that prohibits outgoing TCP connections for the application "SEWManager.exe". You can use the following command for this purpose:

```
netsh.exe advfirewall firewall add rule name="SEWManager.exe"
dir=out program="%ProgramFiles% (x86)\SEW\MotionStudio\SEWMan-
ager.exe" protocol=tcp action=block
```

3.2 Long-term measure

Update to MOVITOOLS® MotionStudio V6.70 as soon as the version is available.

31965520/EN – 04/2024

4 General information

4.1 Disclaimer

This document is intended solely to provide information to our customers. The contents have been created with the greatest care, and efforts are made to ensure that they are as up to date as possible. However, SEW-EURODRIVE accepts no liability for the information provided being correct, complete, or up to date. It is published without recognition of any legal obligation.

The proposed corrective measures are for general informational purposes. Whether or to what extent these are applicable to your application environment is subject to your review of the specific conditions on site.

4.2 Product names and trademarks

The product names mentioned in this documentation are trademarks or registered trademarks of the respective titleholders.

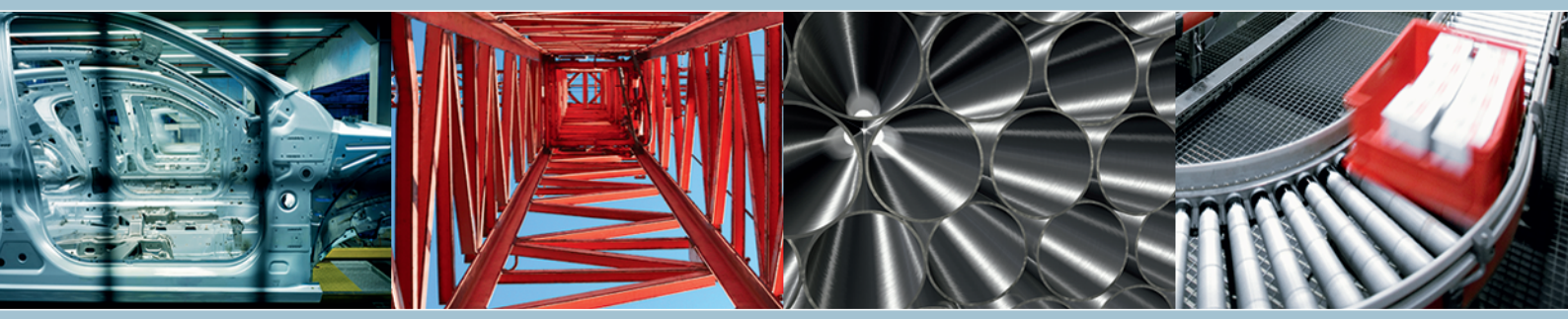
4.3 Copyright notice

4.4 Document history

This customer information is continually updated as new information becomes available, and the most recent version can be found at www.sew.eurodrive.de.

Version	Date	Changes
1	April 15, 2024	Initial document

31965520/EN – 04/2024



SEW-EURODRIVE GmbH & Co KG
Ernst-Blickle-Str. 42
76646 BRUCHSAL
GERMANY
Tel. +49 7251 75-0
Fax +49 7251 75-1970
sew@sew-eurodrive.com
→ www.sew-eurodrive.com