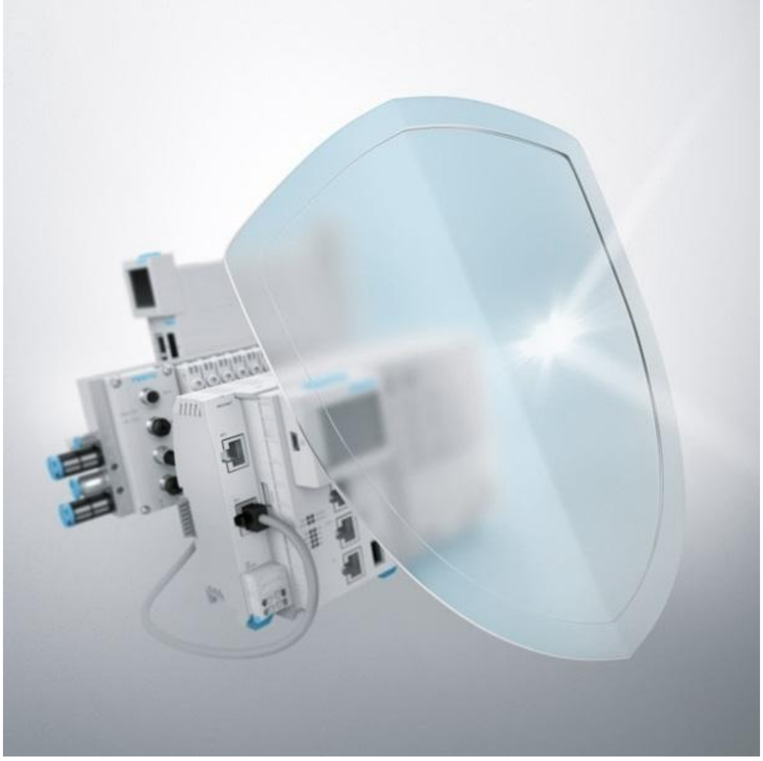
MSE6-C2M/D2M/E2M Incomplete User Documentation of Remote Accessible Functions



fsa-202304

Date
September 05th, 2023

Creator
Festo SE & Co. KG

Version
1.0.0

Festo SE & Co. KG

www.festo.com/psirt
psirt@festo.com
Ruiter Straße 82
73734 Esslingen
GERMANY

Summary

Incomplete user documentation of undocumented, authenticated test mode and further remote accessible functions. The supported features may be covered only partly by the corresponding user documentation.

Festo developed the products according to the respective state of the art. As a result, the protocols used no longer fully meet today's security requirements. The products are designed and developed for use in sealed-off (industrial) networks. If the network is not adequately sealed off, unauthorized access to the product can cause damage or malfunctions, particularly Denial of Service (DoS) or loss of integrity.

Vulnerability Identifier

CVEs: CVE-2023-3634

Severity

8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

Affected Vendors

FESTO

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
Service unit MSE6-C2M: Service unit MSE6-C2M-* all versions affected	Festo:Partnumber:8157908, 8169407, 8169406, 8157912, 8157909, 8157913 Festo:Ordercode:MSE6-C2M-5000-FB44-D-M-RG-BAR-AMI-AGD, MSE6-C2M-5000-FB43-D-M-RG-BAR-M12L4-MQ1-AGD, MSE6-C2M-5000-FB36-D-M-RG-BAR-M12L4-AGD, MSE6-C2M-5000-FB43-D-M-RG-BAR-M12L5-MQ1-AGD, MSE6-C2M-5000-FB44-D-RG-BAR-AMI-AGD, MSE6-C2M-5000-FB36-D-M-RG-BAR-M12L5-AGD	For all CVEs: Update of user documentation in next product version. See section Workarounds and Mitigations.
Service unit MSE6-E2M: Service unit MSE6-E2M-*	Festo:Partnumber:3990296, 2465321, 3992150, 8157911, 8157910 Festo:Ordercode:MSE6-E2M-5000-FB36-AGD, MSE6-	For all CVEs: Update of user documentation in next product version.

Affected Product and Versions	Product Details	Remediation
all versions affected	E2M-5000-FB13-AGD, MSE6-E2M-5000-FB37-AGD, MSE6-E2M-5000-FB44-AGD, MSE6-E2M-5000-FB43-AGD	See section Workarounds and Mitigations.
Energy efficiency module MSE6-D2M: Energy efficiency module MSE6-D2M-* all versions affected	Festo:Partnumber:8085453 Festo:Ordercode:MSE6-D2M-5000-CBUS-S-RG-BAR-VCB-AGD	For all CVEs: Update of user documentation in next product version. See section Workarounds and Mitigations.

Workarounds and Mitigations

Remediations can be found in the table of Affected Products and Recommendations.

Additionally, please refer to the General Recommendations.

Impact and Classification of Vulnerabilities

CVE-2023-3634
In products of the MSE6 product-family by Festo a remote authenticated, low privileged attacker could use functions of undocumented test mode which could lead to a complete loss of confidentiality, integrity and availability.
Weakness: Hidden Functionality (CWE-912)
Base Score: 8.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

General recommendations

Users running communication over an untrusted network who require full protection should switch to an alternative solution such as running the communication over a VPN.

Festo strongly recommends to minimize and protect network access to connected devices with state of the art techniques and processes.

As part of a security strategy, Festo recommends the following general defense measures to reduce the risk of exploits:
- Use devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside
- Use firewalls to protect and separate the control system network from other networks
- Use VPN (Virtual Private Networks) tunnels if remote access is required
- Activate and apply user management and password features
- Use encrypted communication links
- Limit the access to both development and control system by physical means, operating system features, etc.
- Protect both development and control system by using up to date virus detecting solutions

Acknowledgments

Festo SE & Co. KG thanks the following parties for their efforts:

- CERT@VDE for coordination and support with this publication (see: https://cert.vde.com/)

Publisher Details

https://festo.com/psirt
Festo SE & Co. KG, PSIRT, Ruiter Straße 82, 73734 Esslingen Germany, psirt@festo.com
For further security-related issues in Festo products please contact the Festo Product Security Incident Response Team (PSIRT) https://festo.com/psirt

Further References

For further information also refer to:

- VDE-2023-020
- CERT@VDE Security Advisories https://cert.vde.com/en/advisories/vendor/festo/
- CVE entry at Mitre https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3634

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	September 05th, 2023	Initial version

Sharing rules

TLP: WHITE

For the TLP version see: https://www.first.org/tlp

Disclaimer

Festo assumes no liability whatsoever for indirect, collateral, accidental or consequential losses that occur by the distribution and/or use of this document or any losses in connection with the distribution and/or use of this document. All information published in this document is provided free of charge and on good faith by Festo. Insofar as permissible by law, however, none of this information shall establish any warranty, guarantee, commitment or liability on the part of Festo. Note: In no case does these information release the operator or responsible person from the obligation to check the effect on his system or installation before using the information and, in the event of negative consequences, not to use the information.

In addition, the actual general terms and conditions of Festo for delivery, payment and software use shall apply, available under http://www.festo.com.