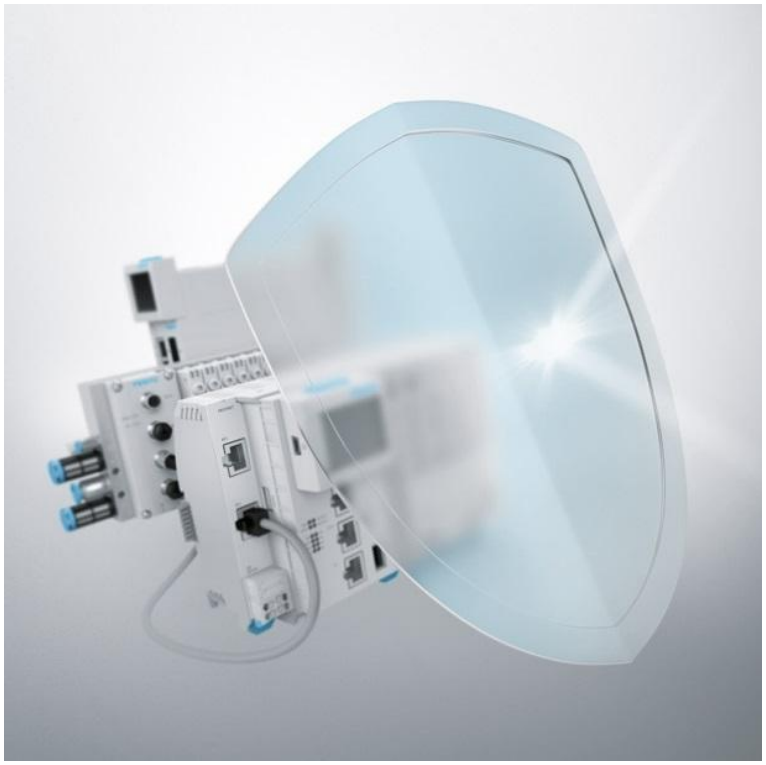
Vulnerable Wibu CodeMeter Runtime in Several Festo Products



fsa-202305

Date
December 05th, 2023

Creator
Festo SE & Co. KG

Version
1.1.0

Festo SE & Co. KG

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

Summary

A vulnerability in the Wibu CodeMeter Runtime, which is part of the installation packages of several Festo products, was found. An attacker exploiting the vulnerability in WIBU CodeMeter Runtime in server mode could gain full access to the affected server via network access without any user interaction. This could lead to remote code execution and escalation of privileges giving full admin access on the host system for an already authenticated user (logged in locally to the PC).

Vulnerability Identifier

CVEs: CVE-2023-3935

Severity

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

Affected Vendors

FESTO, FESTO Didactic

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
Festo Automation Suite: Festo Automation Suite <= 2.6.0.481 affected	Festo:Partnumber:8074657 Festo:Ordercode:FestoAutomationSuite	For all CVEs (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H): Planned Fix in Summer Release 2024
FluidDraw: FluidDraw P6 <= 6.2k affected	Festo:Partnumber:8085496 Festo:Ordercode:FluidDraw	For all CVEs (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H): Update to the latest version.
FluidDraw: FluidDraw 365 <= 7.0a affected	Festo:Partnumber:8085497 Festo:Ordercode:FluidDraw	For all CVEs (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H): Update to the latest version.

Affected Product and Versions	Product Details	Remediation
CIROS Studio / Education: CIROS Studio / Education 6.0.0 - 6.4.6 affected	Festo:Partnumber:8038980	For all CVEs (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/CR:L/IR:L/AR:L): Update CodeMeter Runtime to version >= 7.60c The latest version of CodeMeter Runtime can be downloaded from WIBU System's web site.
CIROS Studio / Education: CIROS Studio / Education 7.0.0 - 7.1.7 affected	Festo:Partnumber:8140772, 8140773	For all CVEs (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/CR:L/IR:L/AR:L): Update CodeMeter Runtime to version >= 7.60c The latest version of CodeMeter Runtime can be downloaded from WIBU System's web site.
FluidSIM: FluidSIM 5 all versions affected		For all CVEs (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/CR:L/IR:L/AR:L): Update CodeMeter Runtime to version >= 7.60c The latest version of CodeMeter Runtime can be downloaded from WIBU System's web site.
FluidSIM: FluidSIM 6 <= 6.1c affected	Festo:Partnumber:8148657, 8148658, 8148659, 8148812, 8148813, 8148814	For all CVEs (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/CR:L/IR:L/AR:L): Update CodeMeter Runtime to version >= 7.60c The latest version of CodeMeter Runtime can be

Affected Product and Versions	Product Details	Remediation
		downloaded from WIBU System's web site.
MES-PC: MES-PC shipped before December 2023 affected		For all CVEs (Score: 9.8; Vectorstring: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/CR:L/IR:L/AR:L): Update CodeMeter Runtime to version >= 7.60c The latest version of CodeMeter Runtime can be downloaded from WIBU System's web site.

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-2023-3935
A heap buffer overflow vulnerability in Wibu CodeMeter Runtime network service up to version 7.60b allows an unauthenticated, remote attacker to achieve RCE and gain full access of the host system.
Weakness: Out-of-bounds Write (CWE-787)
Base Score: 9.8
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/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-2023-036
- CERT@VDE Security Advisories https://cert.vde.com/en/advisories/vendor/festo/

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	November 28th, 2023	Initial version
1.1.0	December 05th, 2023	Removed 'MES4 (v3)', 'MES4 (<=v2)' and 'Energy-PC' from affected products as they do not install WIBU CodeMeter Runtime.

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.