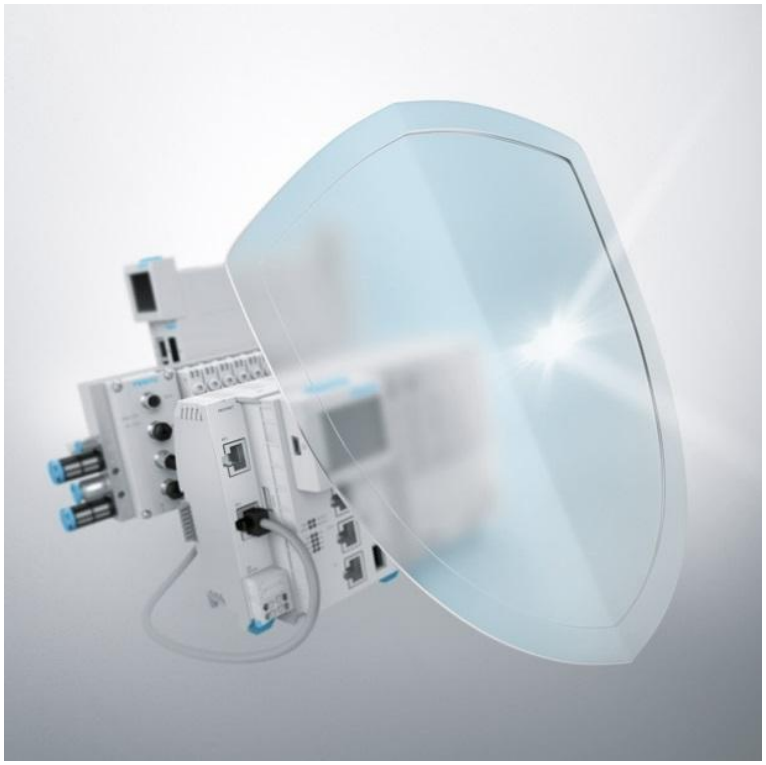
Vulnerable Siemens TIA-Portal in several Festo Didactic Products



FSA-202303

Date
October 17th, 2022

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

A vulnerability was reported in Siemens TIA Portal. TIA Portal is part of the installation packages of several Festo Didactic products.
TP 260 before June 2023 and MES PC based on DELL XE3 contain a vulnerable versions of TIA Portal V15 to V18.
Affected products of TIA Portal contain a path traversal vulnerability that could allow the creation or overwrite of arbitrary files in the engineering system.

Vulnerability Identifier

CVEs: CVE-2023-26293

Severity

7.8 (CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/CR:L/IR:L/AR:L)

Affected Vendors

Festo Didactic

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
TP 260 with TIA-Portal V15 ‹ V17 Update 6 or V18 ‹ V18 Update 1: TP 260 before June 2023 affected	Festo:Partnumber: 8107242	For all CVEs: Update TIA-Portal. Please refer to SSA-116924 for more details.
MES PC with TIA-Portal V15 ‹ V17 Update 6 or V18 ‹ V18 Update 1: MES PC based on DELL XE3 affected		For all CVEs: Update TIA-Portal. Please refer to SSA-116924 for more details.

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-2023-26293
A vulnerability has been identified in Totally Integrated Automation Portal (TIA Portal) V15 (All versions), Totally Integrated Automation Portal (TIA Portal) V16 (All versions), Totally Integrated Automation Portal (TIA Portal) V17 (All versions < V17 Update 6), Totally Integrated Automation Portal (TIA Portal) V18 (All versions < V18 Update 1). Affected products contain a path traversal vulnerability that could allow the creation or overwrite of arbitrary files in the engineering system. If the user is tricked to open a malicious PC system configuration file, an attacker could exploit this vulnerability to achieve arbitrary code execution.
Weakness: Improper Input Validation (CWE-20)
Base Score: 7.8
Vector String: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/CR:L/IR:L/AR:L

General recommendations

As part of a security strategy, Festo recommends the following general defense measures to reduce the risk of exploits:
- Use controllers and 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

Festo strongly recommends to minimize and protect network access to connected devices with state of the art techniques and processes.
For a secure operation follow the recommendations in the product manuals.

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-2023-047
- CERT@VDE Security Advisories https://cert.vde.com/en/advisories/vendor/festo/
- CVE-2023-26293 https://cve.mitre.org/cgi-bin/cvename.cgi?name=2023-26293
- Siemens SSA-116924 https://cert-portal.siemens.com/productcert/pdf/ssa-116924.pdf

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	October 17th, 2022	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.