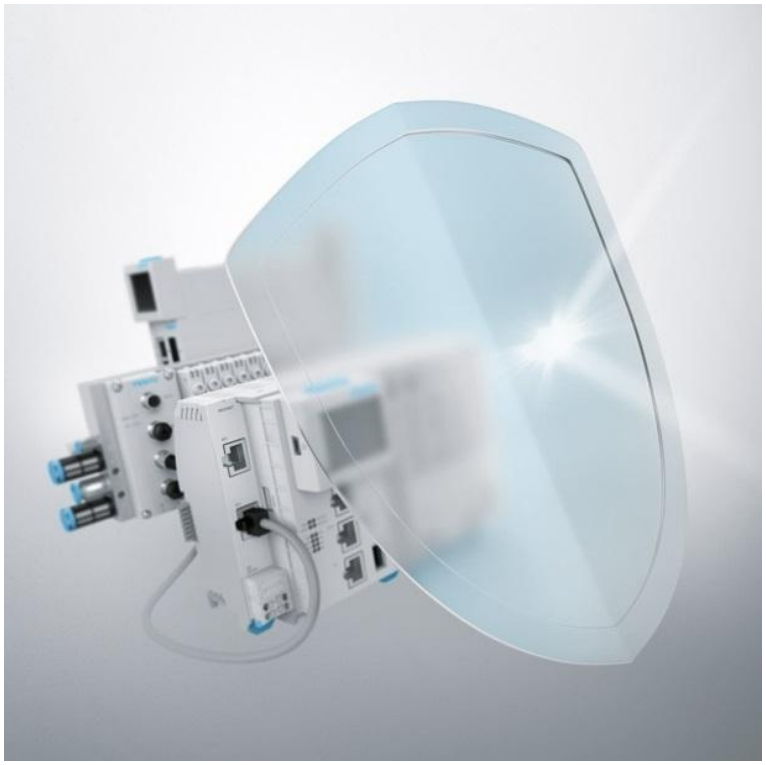
# Several CODESYS vulnerabilities in Festo Automation Suite



**FSA-202601**

Date
February 26th, 2026

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

Starting with Festo Automation Suite (FAS) version 2.8.0.138, the suite is delivered only with a connector to Codesys, rather than including Codesys directly. Prior to this version, Codesys was bundled within the FAS installation. From version 2.8.0.138 onwards, customers are required to download and install Codesys independently.

This change impacts the handling of security vulnerabilities (CVEs) related to Codesys. Any Codesys-related security issues must now be addressed by the customer through their separate Codesys installation. The FAS itself includes only the connector component, which is maintained and updated within the suite.

Please ensure that Codesys is kept up to date independently to mitigate any potential security risks associated with the Codesys software.

The vulnerabilities covered by this advisory have a broad range of impacts ranging from denial-of-service to disclosure or manipulation/deletion of information.

## Vulnerability Identifier

CVEs: CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-5105, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9011, CVE-2019-9012, CVE-2019-9013, CVE-2019-13532, CVE-2019-13538, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2019-19789, CVE-2020-7052, CVE-2020-10245, CVE-2020-11023, CVE-2020-12067, CVE-2020-12068, CVE-2020-12069, CVE-2020-14509, CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-15806, CVE-2020-16233, CVE-2021-21863, CVE-2021-21864, CVE-2021-21865, CVE-2021-21866, CVE-2021-21867, CVE-2021-21868, CVE-2021-21869, CVE-2021-29239, CVE-2021-29240, CVE-2021-29241, CVE-2021-29242, CVE-2021-30186, CVE-2021-30187, CVE-2021-30188, CVE-2021-30190, CVE-2021-30195, CVE-2021-33485, CVE-2021-33486, CVE-2021-34593, CVE-2021-34595, CVE-2021-34596, CVE-2021-36763, CVE-2021-36764, CVE-2021-36765, CVE-2022-1965, CVE-2022-1989, CVE-2022-4046, CVE-2022-4048, CVE-2022-4224, CVE-2022-22508, CVE-2022-22513, CVE-2022-22514, CVE-2022-22515, CVE-2022-22516, CVE-2022-22517, CVE-2022-22519, CVE-2022-30791, CVE-2022-30792, CVE-2022-31805, CVE-2022-31806, CVE-2022-32136, CVE-2022-32137, CVE-2022-32138, CVE-2022-32139, CVE-2022-32140, CVE-2022-32141, CVE-2022-32142, CVE-2022-32143, CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47391, CVE-2022-47392, CVE-2022-47393, CVE-2023-3662, CVE-2023-3663, CVE-2023-3669, CVE-2023-3670, CVE-2023-3935, CVE-2023-6357, CVE-2023-37545, CVE-2023-37546, CVE-2023-37547,

CVE-2023-37548, CVE-2023-37549, CVE-2023-37550, CVE-2023-37551, CVE-2023-37552, CVE-2023-37553, CVE-2023-37554, CVE-2023-37555, CVE-2023-37556, CVE-2023-37557, CVE-2023-37558, CVE-2023-37559, CVE-2023-49675, CVE-2023-49676, CVE-2024-5000, CVE-2024-8175, CVE-2025-0694, CVE-2025-1468, CVE-2025-2595, CVE-2025-41658, CVE-2025-41659

**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,CODESYS

**Affected Products and Remediations**

| Affected Product and Versions | Product Details | Remediation |
|---|---|---|
| CODESYS Development System: Development System 3.0Festo Automation Suite: Festo Automation Suite <2.8.0.138 affected | | For CVE-2025-2595:<br>Starting from Festo Automation Suite version 2.8.0.138, Codesys is no longer bundled with the suite and must be downloaded and installed separately by the customer. To mitigate this vulnerability customers are advised to:<br><br>Download the latest, patched version of Codesys directly from the official Codesys website.<br>Follow the installation and update instructions provided by Codesys to ensure all security fixes are applied.<br>Regularly monitor Codesys security advisories and apply updates promptly.<br>Maintain the Festo Automation Suite connector up to date by installing FAS updates as released by Festo.<br><br>For CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-13532, CVE-2019-13538, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2019-19789, CVE-2019-5105, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9011, CVE-2019-9012, CVE-2019-9013, CVE-2020-10245, CVE-2020-11023, |

| Affected Product and Versions | Product Details | Remediation |
|---|---|---|
| | | CVE-2020-12067, CVE-2020-12068, CVE-2020-12069, CVE-2020-14509, CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-15806, CVE-2020-16233, CVE-2020-7052, CVE-2021-21863, CVE-2021-21864, CVE-2021-21865, CVE-2021-21866, CVE-2021-21867, CVE-2021-21868, CVE-2021-21869, CVE-2021-29239, CVE-2021-29240, CVE-2021-29241, CVE-2021-29242, CVE-2021-30186, CVE-2021-30187, CVE-2021-30188, CVE-2021-30190, CVE-2021-30195, CVE-2021-33485, CVE-2021-33486, CVE-2021-34593, CVE-2021-34595, CVE-2021-34596, CVE-2021-36763, CVE-2021-36764, CVE-2021-36765, CVE-2022-1965, CVE-2022-1989, CVE-2022-22508, CVE-2022-22513, CVE-2022-22514, CVE-2022-22515, CVE-2022-22516, CVE-2022-22517, CVE-2022-22519, CVE-2022-30791, CVE-2022-30792, CVE-2022-31805, CVE-2022-31806, CVE-2022-32136, CVE-2022-32137, CVE-2022-32138, CVE-2022-32139, CVE-2022-32140, CVE-2022-32141, CVE-2022-32142, CVE-2022-32143, CVE-2022-4046, CVE-2022-4048, CVE-2022-4224, CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47391, CVE-2022-47392, CVE-2022-47393, CVE-2023-3662, CVE-2023-3663, CVE-2023-3669, CVE-2023-3670, CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550, CVE-2023-37551, CVE-2023-37552, CVE-2023-37553, CVE-2023-37554, CVE-2023-37555, CVE-2023-37556, CVE-2023-37557, CVE-2023-37558, CVE-2023-37559, CVE-2023-3935, CVE-2023-49675, CVE-2023-49676, CVE-2023-6357, CVE-2024-5000, CVE-2024-8175, CVE-2025-0694, CVE-2025-1468, CVE-2025-41658, CVE-2025-41659:<br>Starting from Festo Automation Suite version 2.8.0.138, Codesys is no longer bundled with the suite and must be downloaded and installed separately by the customer. To mitigate this vulnerability customers are advised to: |

| Affected Product and Versions | Product Details | Remediation |
|---|---|---|
| | | Download the latest, patched version of Codesys directly from the official Codesys website.<br>Follow the installation and update instructions provided by Codesys to ensure all security fixes are applied.<br>Regularly monitor Codesys security advisories and apply updates promptly.<br>Maintain the Festo Automation Suite connector up to date by installing FAS updates as released by Festo. |
| CODESYS Development System: Development System 3.5.16.10Festo Automation Suite: Festo Automation Suite <2.8.0.138 affected | | For CVE-2025-2595:<br>Starting from Festo Automation Suite version 2.8.0.138, Codesys is no longer bundled with the suite and must be downloaded and installed separately by the customer. To mitigate this vulnerability customers are advised to:<br><br>Download the latest, patched version of Codesys directly from the official Codesys website.<br>Follow the installation and update instructions provided by Codesys to ensure all security fixes are applied.<br>Regularly monitor Codesys security advisories and apply updates promptly.<br>Maintain the Festo Automation Suite connector up to date by installing FAS updates as released by Festo.<br><br>For CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-13532, CVE-2019-13538, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2019-19789, CVE-2019-5105, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9011, CVE-2019-9012, CVE-2019-9013, CVE-2020-10245, CVE-2020-11023, CVE-2020-12067, CVE-2020-12068, CVE-2020-12069, CVE-2020-14509, CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-15806, CVE-2020-16233, CVE-2020-7052, CVE-2021-21863, CVE-2021-21864, CVE-2021-21865, CVE-2021-21866, CVE-2021-21867, CVE-2021-21868, CVE-2021-21869, CVE-2021-29239, CVE-2021-29240, CVE-2021-29241, CVE-2021-29242, CVE-2021-30186, CVE-2021-30187, |

| Affected Product and Versions | Product Details | Remediation |
|---|---|---|
| | | CVE-2021-30188, CVE-2021-30190, CVE-2021-30195, CVE-2021-33485, CVE-2021-33486, CVE-2021-34593, CVE-2021-34595, CVE-2021-34596, CVE-2021-36763, CVE-2021-36764, CVE-2021-36765, CVE-2022-1965, CVE-2022-1989, CVE-2022-22508, CVE-2022-22513, CVE-2022-22514, CVE-2022-22515, CVE-2022-22516, CVE-2022-22517, CVE-2022-22519, CVE-2022-30791, CVE-2022-30792, CVE-2022-31805, CVE-2022-31806, CVE-2022-32136, CVE-2022-32137, CVE-2022-32138, CVE-2022-32139, CVE-2022-32140, CVE-2022-32141, CVE-2022-32142, CVE-2022-32143, CVE-2022-4046, CVE-2022-4048, CVE-2022-4224, CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47391, CVE-2022-47392, CVE-2022-47393, CVE-2023-3662, CVE-2023-3663, CVE-2023-3669, CVE-2023-3670, CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550, CVE-2023-37551, CVE-2023-37552, CVE-2023-37553, CVE-2023-37554, CVE-2023-37555, CVE-2023-37556, CVE-2023-37557, CVE-2023-37558, CVE-2023-37559, CVE-2023-3935, CVE-2023-49675, CVE-2023-49676, CVE-2023-6357, CVE-2024-5000, CVE-2024-8175, CVE-2025-0694, CVE-2025-1468, CVE-2025-41658, CVE-2025-41659:<br>Starting from Festo Automation Suite version 2.8.0.138, Codesys is no longer bundled with the suite and must be downloaded and installed separately by the customer. To mitigate this vulnerability customers are advised to:<br><br>Download the latest, patched version of Codesys directly from the official Codesys website.<br>Follow the installation and update instructions provided by Codesys to ensure all security fixes are applied.<br>Regularly monitor Codesys security advisories and apply updates promptly. |

| Affected Product and Versions | Product Details | Remediation |
|---|---|---|
| | | Maintain the Festo Automation Suite connector up to date by installing FAS updates as released by Festo. |
| CODESYS Development System: Development System 3.0Festo Automation Suite: Festo Automation Suite 2.8.0.137 affected | | For CVE-2025-2595:<br>Starting from Festo Automation Suite version 2.8.0.138, Codesys is no longer bundled with the suite and must be downloaded and installed separately by the customer. To mitigate this vulnerability customers are advised to:<br><br>Download the latest, patched version of Codesys directly from the official Codesys website.<br>Follow the installation and update instructions provided by Codesys to ensure all security fixes are applied.<br>Regularly monitor Codesys security advisories and apply updates promptly.<br>Maintain the Festo Automation Suite connector up to date by installing FAS updates as released by Festo.<br><br>For CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-13532, CVE-2019-13538, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2019-19789, CVE-2019-5105, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9011, CVE-2019-9012, CVE-2019-9013, CVE-2020-10245, CVE-2020-11023, CVE-2020-12067, CVE-2020-12068, CVE-2020-12069, CVE-2020-14509, CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-15806, CVE-2020-16233, CVE-2020-7052, CVE-2021-21863, CVE-2021-21864, CVE-2021-21865, CVE-2021-21866, CVE-2021-21867, CVE-2021-21868, CVE-2021-21869, CVE-2021-29239, CVE-2021-29240, CVE-2021-29241, CVE-2021-29242, CVE-2021-30186, CVE-2021-30187, CVE-2021-30188, CVE-2021-30190, CVE-2021-30195, CVE-2021-33485, CVE-2021-33486, CVE-2021-34593, CVE-2021-34595, CVE-2021-34596, CVE-2021-36763, CVE-2021-36764, CVE-2021-36765, CVE-2022-1965, CVE-2022-1989, CVE-2022-22508, CVE-2022-22513, CVE-2022-22514, CVE-2022-22515, CVE-2022-22516, CVE-2022-22517, CVE-2022-22519, CVE-2022-30791, |

| Affected Product and Versions | Product Details | Remediation |
|---|---|---|
| | | CVE-2022-30792, CVE-2022-31805, CVE-2022-31806, CVE-2022-32136, CVE-2022-32137, CVE-2022-32138, CVE-2022-32139, CVE-2022-32140, CVE-2022-32141, CVE-2022-32142, CVE-2022-32143, CVE-2022-4046, CVE-2022-4048, CVE-2022-4224, CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47391, CVE-2022-47392, CVE-2022-47393, CVE-2023-3662, CVE-2023-3663, CVE-2023-3669, CVE-2023-3670, CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550, CVE-2023-37551, CVE-2023-37552, CVE-2023-37553, CVE-2023-37554, CVE-2023-37555, CVE-2023-37556, CVE-2023-37557, CVE-2023-37558, CVE-2023-37559, CVE-2023-3935, CVE-2023-49675, CVE-2023-49676, CVE-2023-6357, CVE-2024-5000, CVE-2024-8175, CVE-2025-0694, CVE-2025-1468, CVE-2025-41658, CVE-2025-41659:<br>Starting from Festo Automation Suite version 2.8.0.138, Codesys is no longer bundled with the suite and must be downloaded and installed separately by the customer. To mitigate this vulnerability customers are advised to:<br><br>Download the latest, patched version of Codesys directly from the official Codesys website.<br>Follow the installation and update instructions provided by Codesys to ensure all security fixes are applied.<br>Regularly monitor Codesys security advisories and apply updates promptly.<br>Maintain the Festo Automation Suite connector up to date by installing FAS updates as released by Festo. |
| CODESYS Development System: Development System 3.5.16.10Festo | | For CVE-2025-2595:<br>Starting from Festo Automation Suite version 2.8.0.138, Codesys is no longer bundled with the suite and must be downloaded and installed separately by the customer. To mitigate this vulnerability customers are advised to: |

| Affected Product and Versions | Product Details | Remediation |
|---|---|---|
| Automation Suite: Festo Automation Suite 2.8.0.137 affected | | Download the latest, patched version of Codesys directly from the official Codesys website.<br>Follow the installation and update instructions provided by Codesys to ensure all security fixes are applied.<br>Regularly monitor Codesys security advisories and apply updates promptly.<br>Maintain the Festo Automation Suite connector up to date by installing FAS updates as released by Festo.<br><br>For CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-13532, CVE-2019-13538, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2019-19789, CVE-2019-5105, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9011, CVE-2019-9012, CVE-2019-9013, CVE-2020-10245, CVE-2020-11023, CVE-2020-12067, CVE-2020-12068, CVE-2020-12069, CVE-2020-14509, CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-15806, CVE-2020-16233, CVE-2020-7052, CVE-2021-21863, CVE-2021-21864, CVE-2021-21865, CVE-2021-21866, CVE-2021-21867, CVE-2021-21868, CVE-2021-21869, CVE-2021-29239, CVE-2021-29240, CVE-2021-29241, CVE-2021-29242, CVE-2021-30186, CVE-2021-30187, CVE-2021-30188, CVE-2021-30190, CVE-2021-30195, CVE-2021-33485, CVE-2021-33486, CVE-2021-34593, CVE-2021-34595, CVE-2021-34596, CVE-2021-36763, CVE-2021-36764, CVE-2021-36765, CVE-2022-1965, CVE-2022-1989, CVE-2022-22508, CVE-2022-22513, CVE-2022-22514, CVE-2022-22515, CVE-2022-22516, CVE-2022-22517, CVE-2022-22519, CVE-2022-30791, CVE-2022-30792, CVE-2022-31805, CVE-2022-31806, CVE-2022-32136, CVE-2022-32137, CVE-2022-32138, CVE-2022-32139, CVE-2022-32140, CVE-2022-32141, CVE-2022-32142, CVE-2022-32143, CVE-2022-4046, CVE-2022-4048, CVE-2022-4224, CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, |

| Affected Product and Versions | Product Details | Remediation |
|---|---|---|
| | | CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47391, CVE-2022-47392, CVE-2022-47393, CVE-2023-3662, CVE-2023-3663, CVE-2023-3669, CVE-2023-3670, CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550, CVE-2023-37551, CVE-2023-37552, CVE-2023-37553, CVE-2023-37554, CVE-2023-37555, CVE-2023-37556, CVE-2023-37557, CVE-2023-37558, CVE-2023-37559, CVE-2023-3935, CVE-2023-49675, CVE-2023-49676, CVE-2023-6357, CVE-2024-5000, CVE-2024-8175, CVE-2025-0694, CVE-2025-1468, CVE-2025-41658, CVE-2025-41659:<br>Starting from Festo Automation Suite version 2.8.0.138, Codesys is no longer bundled with the suite and must be downloaded and installed separately by the customer. To mitigate this vulnerability customers are advised to:<br><br>Download the latest, patched version of Codesys directly from the official Codesys website.<br>Follow the installation and update instructions provided by Codesys to ensure all security fixes are applied.<br>Regularly monitor Codesys security advisories and apply updates promptly.<br>Maintain the Festo Automation Suite connector up to date by installing FAS updates as released by Festo. |
| Festo Automation Suite:<br>Festo Automation Suite 2.8.0.138 affected | Festo:Partnumber: 8074657<br><br>Festo:Ordercode:8074657 | :<br>Remediation is missing! Please specify the remediations for the product!<br>See section Workarounds and Mitigations. |

## Workarounds and Mitigations

Festo has identified the following compensatory measures to reduce the risk:

- For CVE-2010-5250, CVE-2017-3735, CVE-2018-0739, CVE-2018-10612, CVE-2018-20025, CVE-2018-20026, CVE-2019-13532, CVE-2019-13538, CVE-2019-13542, CVE-2019-13548, CVE-2019-18858, CVE-2019-19789, CVE-2019-5105, CVE-2019-9008, CVE-2019-9009, CVE-2019-9010, CVE-2019-9011, CVE-2019-9012, CVE-2019-9013, CVE-2020-10245, CVE-2020-11023, CVE-2020-12067, CVE-2020-12068, CVE-2020-12069, CVE-2020-14509, CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-15806, CVE-2020-16233, CVE-2020-7052, CVE-2021-21863, CVE-2021-21864, CVE-2021-21865, CVE-2021-21866, CVE-2021-21867, CVE-2021-21868, CVE-2021-21869, CVE-2021-29239, CVE-2021-29240, CVE-2021-29241, CVE-2021-29242, CVE-2021-30186, CVE-2021-30187, CVE-2021-30188, CVE-2021-30190, CVE-2021-30195, CVE-2021-33485, CVE-2021-33486, CVE-2021-34593, CVE-2021-34595, CVE-2021-34596, CVE-2021-36763, CVE-2021-36764, CVE-2021-36765, CVE-2022-1965, CVE-2022-1989, CVE-2022-22508, CVE-2022-22513, CVE-2022-22514, CVE-2022-22515, CVE-2022-22516, CVE-2022-22517, CVE-2022-22519, CVE-2022-30791, CVE-2022-30792, CVE-2022-31805, CVE-2022-31806, CVE-2022-32136, CVE-2022-32137, CVE-2022-32138, CVE-2022-32139, CVE-2022-32140, CVE-2022-32141, CVE-2022-32142, CVE-2022-32143, CVE-2022-4046, CVE-2022-4048, CVE-2022-4224, CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47391, CVE-2022-47392, CVE-2022-47393, CVE-2023-3662, CVE-2023-3663, CVE-2023-3669, CVE-2023-3670, CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550, CVE-2023-37551, CVE-2023-37552, CVE-2023-37553, CVE-2023-37554, CVE-2023-37555, CVE-2023-37556, CVE-2023-37557, CVE-2023-37558, CVE-2023-37559, CVE-2023-3935, CVE-2023-49675, CVE-2023-49676, CVE-2023-6357, CVE-2024-5000, CVE-2024-8175, CVE-2025-0694, CVE-2025-1468, CVE-2025-41658, CVE-2025-41659: Starting from Festo Automation Suite version 2.8.0.138, Codesys is no longer bundled with the suite and must be downloaded and installed separately by the customer. To mitigate this vulnerability customers are advised to:

  Download the latest, patched version of Codesys directly from the official Codesys website.
  Follow the installation and update instructions provided by Codesys to ensure all security fixes are applied.
  Regularly monitor Codesys security advisories and apply updates promptly.
  Maintain the Festo Automation Suite connector up to date by installing FAS updates as released by Festo.
- For CVE-2025-2595: Starting from Festo Automation Suite version 2.8.0.138, Codesys is no longer bundled with the suite and must be downloaded and installed separately by the

customer. To mitigate this vulnerability customers are advised to:

Download the latest, patched version of Codesys directly from the official Codesys website.
Follow the installation and update instructions provided by Codesys to ensure all security fixes are applied.
Regularly monitor Codesys security advisories and apply updates promptly.
Maintain the Festo Automation Suite connector up to date by installing FAS updates as released by Festo.

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

Additionally, please refer to the General Recommendations.

**Impact and Classification of Vulnerabilities**

Only showing details of vulnerabilities with critical severity, please see in the list of Vulnerability Identifier for a complete list.

CVE-2018-10612
In 3S-Smart Software Solutions GmbH CODESYS Control V3 products prior to version 3.5.14.0, user access management and communication encryption is not enabled by default, which could allow an attacker access to the device and sensitive information, including user credentials.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-284: Improper Access Control |

CVE-2019-9010
An issue was discovered in 3S-Smart CODESYS V3 products. The CODESYS Gateway does not correctly verify the ownership of a communication channel. All variants of the following CODESYS V3 products in all versions prior to v3.5.14.20 that contain the CmpGateway component are affected, regardless of the CPU type or operating system: CODESYS Control for BeagleBone, CODESYS Control for emPC-A/iMX6, CODESYS Control for IOT2000, CODESYS Control for Linux, CODESYS Control for PFC100, CODESYS Control for PFC200, CODESYS Control for Raspberry Pi, CODESYS Control V3 Runtime System Toolkit, CODESYS Gateway V3, CODESYS V3 Development System.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-284: Improper Access Control |

CVE-2019-13548
CODESYS V3 web server, all versions prior to 3.5.14.10, allows an attacker to send specially crafted http or https requests which could cause a stack overflow and create a denial-of-service condition or allow remote code execution.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-121: Stack-based Buffer Overflow |

CVE-2019-18858
CODESYS 3 web server before 3.5.15.20, as distributed with CODESYS Control runtime systems, has a Buffer Overflow.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') |

CVE-2020-10245
CODESYS V3 web server before 3.5.15.40, as used in CODESYS Control runtime systems, has a buffer overflow.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-787: Out-of-bounds Write |

CVE-2020-14509
Multiple memory corruption vulnerabilities exist in CodeMeter (All versions prior to 7.10) where the packet parser mechanism does not verify length fields. An attacker could send specially crafted packets to exploit these vulnerabilities.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-805: Buffer Access with Incorrect Length Value |

CVE-2020-14517
Protocol encryption can be easily broken for CodeMeter (All versions prior to 6.90 are affected, including Version 6.90 or newer only if CodeMeter Runtime is running as server) and the server accepts external connections, which may allow an attacker to remotely communicate with the CodeMeter API.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-326: Inadequate Encryption Strength |

CVE-2021-30188
CODESYS V2 runtime system SP before 2.4.7.55 has a Stack-based Buffer Overflow.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-787: Out-of-bounds Write |

CVE-2021-30190
CODESYS V2 Web-Server before 1.1.9.20 has Improper Access Control.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-306: Missing Authentication for Critical Function |

CVE-2021-33485
CODESYS Control Runtime system before 3.5.17.10 has a Heap-based Buffer Overflow.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-787: Out-of-bounds Write |

CVE-2022-31806
In CODESYS V2 PLCWinNT and Runtime Toolkit 32 in versions prior to V2.4.7.57 password protection

is not enabled by default and there is no information or prompt to enable password protection at login in case no password is set at the controller.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-1188: Initialization of a Resource with an Insecure Default |

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.

| | |
|---|---|
| **CVSS v3.1 Base Score** | 9.8 |
| **CVSS v3.1 Vector** | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |
| **CWE** | CWE-787: Out-of-bounds Write |

**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 systems by using up-to-date virus detection solutions.

Festo strongly recommends minimizing and protecting network access to connected devices with state-of-the-art techniques and processes.
To ensure 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://certvde.com)

**Publisher Details**

https://www.festo.com
psirt@festo.com
For further security-related issues in Festo products please contact the Festo Product Security Incident Response Team (PSIRT) https://www.festo.com/psirt

**Further References**

For further information also refer to:

- CERT@VDE Security Advisories https://certvde.com/en/advisories/vendor/festo/
- FSA-202601: Several CODESYS vulnerabilities in Festo Automation Suite - CSAF https://festo.csaf-tp.certvde.com/.well-known/csaf/white/2026/fsa-202601.json
- FSA-202601: Several CODESYS vulnerabilities in Festo Automation Suite - HTML https://certvde.com/en/advisories/VDE-2025-108
- https://nvd.nist.gov/vuln/detail/CVE-2025-2595 https://www.cve.org/CVERecord?id=CVE-2025-2595

**Revision History**

| Version | Date of the revision | Summary of the revision |
|---|---|---|
| 1.0.0 | February 26th, 2026 | 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 this 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 for delivery, payment and software use of Festo, available under http://www.festo.com and the special provisions for the use of Festo Security Advisory available at https://www.festo.com/psirt shall apply.