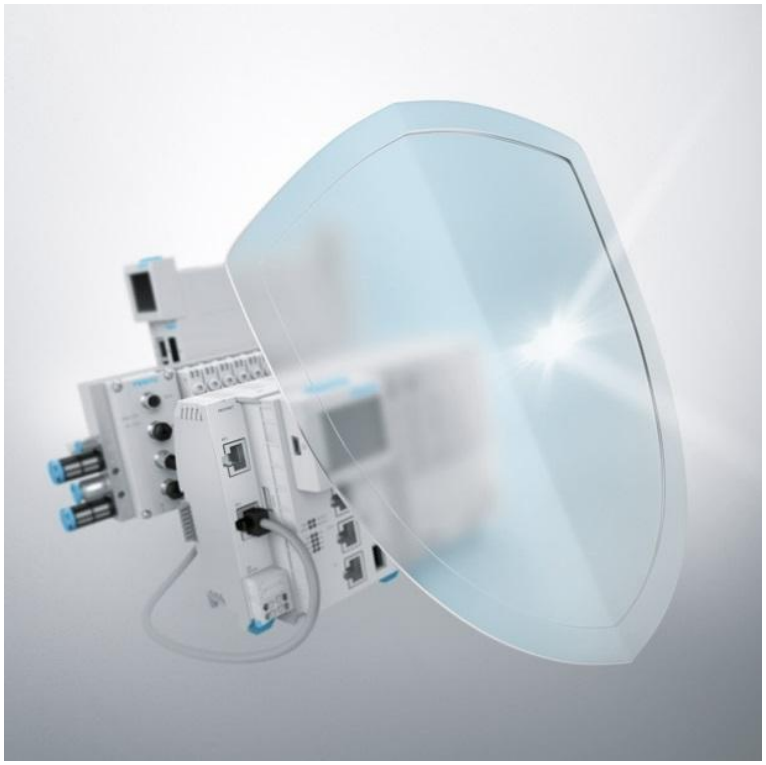
Two critical PHP vulnerabilities in several Festo Didactic products



FSA-202603

Date
November 05th, 2026

Creator
Festo SE & Co. KG

Version
2.0.0

Festo SE & Co. KG

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

Summary

Festo Didactic FactoryViews and MES4 deployed along with xampp bundle an Apache web server with PHP. The bundled version of PHP is vulnerable to the two critical vulnerabilities CVE-2026-109618 and CVE-2026-109619 (commonly referred to as PHP2Shell). These vulnerabilities allow an attacker to remotely execute code on the FactoryViews or xampp host system.

A successful attack on a vulnerable PHP installation allows the attacker to remotely execute malicious code on the FactoryViews or xampp host system with the privileges of the user account running the server application.

Vulnerability Identifier

CVEs: CVE-2026-109618, CVE-2026-109619

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 Didactic

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
FactoryViews: FactoryViews <= 1.12.1 affected		For CVE-2026-109618, CVE-2026-109619: Install patch 1.12.2 through the "Versions" page of the FactoryViews control panel on version 1.12.0 or 1.12.1. Versions of FactoryViews prior to 1.12 must first be updated to 1.12 available for download here: https://www.festo.com/de/de/support-portal-specific?query=factoryviews&groupId=4&productName=factoryviews&documentId=659952
MES4: MES4 with xampp		

Affected Product and Versions	Product Details	Remediation
all versions affected		For CVE-2026-109618, CVE-2026-109619: See section Workarounds and Mitigations.

Workarounds and Mitigations

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

- For CVE-2026-109618: The xampp versions installed with older deployments of MES4 run PHP versions up to 7.3. These version are out-of-support and no patches have been made available.
  Users can apply the mitigation measures recommended by the PHP foundation:
  Set memory_limit=-1 in php.ini.
  Users might also consider adding firewall rules to the Windows host system which restrict communication with httpd.exe from sources other than the HMI panels of manual workstations.
- For CVE-2026-109619: The xampp versions installed with older deployments of MES4 run PHP versions up to 7.3. These version are out-of-support and no patches have been made available.
  Users can apply the mitigation measures recommended by the PHP foundation:
  Set "session.upload_progress.enabled=0" in php.ini.
  Additionally, the setting "MaxConnectionsPerChild 1" can be added to the end of httpd-xampp.conf. Note that this will have a significant negative impact on performance.
  Users might also consider adding firewall rules to the Windows host system which restrict communication with httpd.exe from sources other than the HMI panels of manual workstations.

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-2026-109618
PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in

an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE).

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
CVSS v4.0 Base Score	9.2
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-416: Use After Free

CVE-2026-109619
PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE).

CVSS v3.1 Base Score	8.1
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	9.2
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-416: Use After Free

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

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 Advisory https://certvde.com/en/advisories/vendor/festo/
- FSA-202603: Two critical PHP vulnerabilities in several Festo Didactic products - CSAF https://festo.csaf-tp.certvde.com/.well-known/csaf/white/2026/fsa-202603.json
- FSA-202603: Two critical PHP vulnerabilities in several Festo Didactic products - HTML https://certvde.com/en/advisories/VDE-2026-139

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	November 02nd, 2026	Initial Revision

Version	Date of the revision	Summary of the revision
2.0.0	November 05th, 2026	Adjusted information about vendor fix for FactoryViews

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.