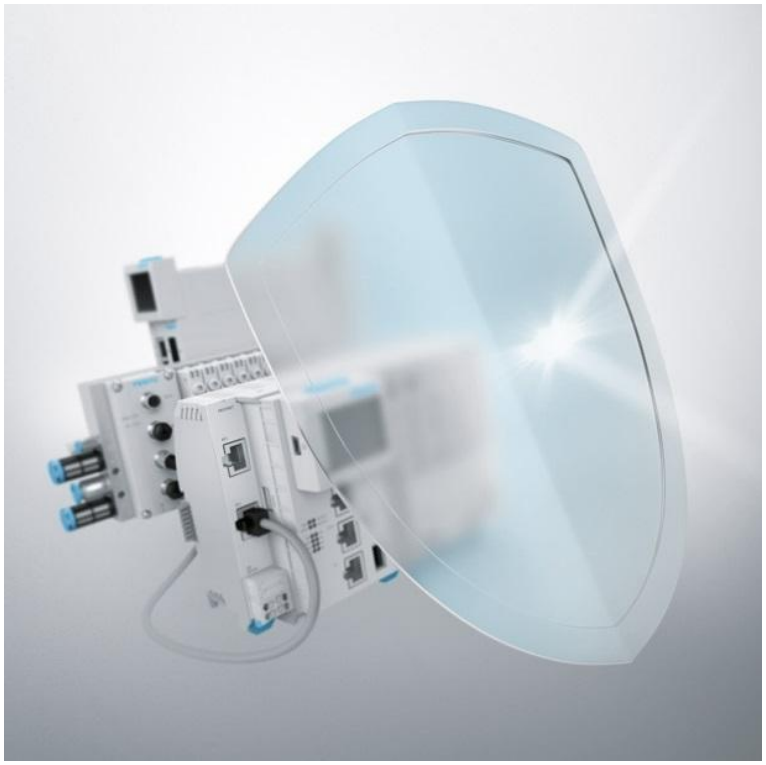
# Several Vulnerabilities in FactoryViews <= 1.5.2



**FSA-202302**

Date
January 11th, 2024

Creator
Festo SE & Co. KG

Version
1.0.1

**Festo SE & Co. KG**

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

## Summary

FactoryViews bundles many third-party applications which are used in background processes to provide the software's features. From time to time, vulnerabilities in these bundled applications are discovered. These are typically fixed in newer versions of FactoryViews by updating the bundled applications.

FactoryViews versions up to and including 1.5.2 contain around 200 such vulnerabilities listed in this advisory.
Version 1.6.0 is a security rollup release which includes updates to all bundled applications and fixes these vulnerabilities.

At this time, FactoryViews Lite cannot be updated beyond version 1.1.
FactoryViews 1.7 will unify non-Lite and Lite versions and fix these vulnerabilities for users of FactoryViews Lite.

The vulnerabilities covered by this advisory have a broad range of impacts ranging from denial-of-service to disclosure or manipulation/deletion of information.
Given the intended purpose of FactoryViews as a didactic tool in controlled lab environments, separate from productive systems, it never comes into contact with sensitive information. Therefore the impact is reduced to limited availability of the system.
To further reduce the risk due to loss of information, users should make use of the built-in backup feature to safeguard important configurations needed for lessons.

## Vulnerability Identifier

CVEs: CVE-2006-20001, CVE-2016-3078, CVE-2016-5385, CVE-2018-12882, CVE-2018-14851, CVE-2018-14883, CVE-2018-17082, CVE-2018-19518, CVE-2018-19935, CVE-2019-9020, CVE-2019-9021, CVE-2019-9022, CVE-2019-9023, CVE-2019-9024, CVE-2019-9025, CVE-2019-9637, CVE-2019-9638, CVE-2019-9639, CVE-2019-9640, CVE-2019-9641, CVE-2019-11034, CVE-2019-11035, CVE-2019-11036, CVE-2019-11039, CVE-2019-11040, CVE-2019-11041, CVE-2019-11042, CVE-2019-11043, CVE-2019-11044, CVE-2019-11045, CVE-2019-11046, CVE-2019-11047, CVE-2019-11048, CVE-2019-11049, CVE-2019-11050, CVE-2019-20454, CVE-2020-7059, CVE-2020-7060, CVE-2020-7061, CVE-2020-7062, CVE-2020-7063, CVE-2020-7064, CVE-2020-7065, CVE-2020-7066, CVE-2020-7068, CVE-2020-7069, CVE-2020-7070, CVE-2020-7071, CVE-2020-28948, CVE-2020-28949, CVE-2020-36193, CVE-2021-2007, CVE-2021-2011, CVE-2021-2022, CVE-2021-2032, CVE-2021-2144, CVE-2021-2154, CVE-2021-2166, CVE-2021-2174, CVE-2021-2180, CVE-2021-2194, CVE-2021-2372, CVE-2021-2389, CVE-2021-3807, CVE-2021-3918, CVE-2021-21702, CVE-2021-21703, CVE-2021-21704, CVE-2021-21705, CVE-2021-21706, CVE-2021-21707, CVE-2021-21708, CVE-2021-22883, CVE-2021-22884, CVE-2021-22918, CVE-2021-22921, CVE-2021-22930, CVE-2021-22931, CVE-2021-22939, CVE-2021-22940, CVE-2021-22959, CVE-2021-22960, CVE-2021-23362, CVE-2021-27290, CVE-2021-27928, CVE-2021-32803, CVE-2021-32804, CVE-2021-35604, CVE-2021-37701, CVE-2021-37712,

CVE-2021-37713, CVE-2021-39134, CVE-2021-39135, CVE-2021-44531, CVE-2021-44532, CVE-2021-44533, CVE-2021-46661, CVE-2021-46662, CVE-2021-46663, CVE-2021-46664, CVE-2021-46665, CVE-2021-46666, CVE-2021-46667, CVE-2021-46668, CVE-2021-46669, CVE-2022-1586, CVE-2022-1587, CVE-2022-21595, CVE-2022-21824, CVE-2022-23807, CVE-2022-23808, CVE-2022-27376, CVE-2022-27377, CVE-2022-27378, CVE-2022-27379, CVE-2022-27380, CVE-2022-27381, CVE-2022-27382, CVE-2022-27383, CVE-2022-27384, CVE-2022-27385, CVE-2022-27386, CVE-2022-27387, CVE-2022-27444, CVE-2022-27445, CVE-2022-27446, CVE-2022-27447, CVE-2022-27448, CVE-2022-27449, CVE-2022-27451, CVE-2022-27452, CVE-2022-27455, CVE-2022-27456, CVE-2022-27457, CVE-2022-27458, CVE-2022-31625, CVE-2022-31626, CVE-2022-31628, CVE-2022-31629, CVE-2022-32081, CVE-2022-32082, CVE-2022-32083, CVE-2022-32084, CVE-2022-32085, CVE-2022-32086, CVE-2022-32087, CVE-2022-32088, CVE-2022-32089, CVE-2022-32091, CVE-2022-32212, CVE-2022-32213, CVE-2022-32214, CVE-2022-32215, CVE-2022-32222, CVE-2022-32223, CVE-2022-35255, CVE-2022-35256, CVE-2022-36313, CVE-2022-36760, CVE-2022-37436, CVE-2022-43548, CVE-2022-47015, CVE-2023-0567, CVE-2023-0568, CVE-2023-0662, CVE-2023-23918, CVE-2023-23919, CVE-2023-23920, CVE-2023-23936, CVE-2023-24807, CVE-2023-25690, CVE-2023-25727, CVE-2023-27522

### Severity

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

### Affected Vendors

Festo Didactic SE

### Affected Products and Remediations

| Affected Product and Versions | Product Details | Remediation |
|---|---|---|
| FactoryViews:<br>FactoryViews (non-Lite) < v1.6.0 affected | | For all CVEs:<br>Upgrade to FactoryViews 1.6.0.<br>See the upgrade guide under "Further references" for information on how to upgrade. |
| FactoryViews:<br>FactoryViews Lite affected | | For all CVEs:<br>An update for FactoryViews Lite is not yet available. This advisory will be updated when a patch is released. |

### 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**

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

CVE-2016-3078
Multiple integer overflows in php_zip.c in the zip extension in PHP before 7.0.6 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted call to (1) getFromIndex or (2) getFromName in the ZipArchive class.
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/AR:L/IR:L/CR:L
CVE-2018-12882
exif_read_from_impl in ext/exif/exif.c in PHP 7.2.x through 7.2.7 allows attackers to trigger a use-after-free (in exif_read_from_file) because it closes a stream that it is not responsible for closing. The vulnerable code is reachable through the PHP exif_read_data function.
Base Score: 9.8
Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/AR:L/IR:L/CR:L
CVE-2019-9020
An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.
Base Score: 9.8
Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/AR:L/IR:L/CR:L
CVE-2019-9021
An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.
Base Score: 9.8
Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/AR:L/IR:L/CR:L
CVE-2019-9023
An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c,

ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.
Base Score: 9.8
Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/AR:L/IR:L/CR:L
CVE-2019-9025
An issue was discovered in PHP 7.3.x before 7.3.1. An invalid multibyte string supplied as an argument to the mb_split() function in ext/mbstring/php_mbregex.c can cause PHP to execute memcpy() with a negative argument, which could read and write past buffers allocated for the data.
Base Score: 9.8
Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/AR:L/IR:L/CR:L
CVE-2019-9641
An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.
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/AR:L/IR:L/CR:L
CVE-2021-3918
json-schema is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
Weakness: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') (CWE-1321)
Base Score: 9.8
Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/AR:L/IR:L/CR:L
CVE-2021-22930
Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to a use after free attack where an attacker might be able to exploit the memory corruption, to change process behavior.
Weakness: Use After Free (CWE-416)
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/AR:L/IR:L/CR:L
CVE-2021-22931
Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to Remote Code Execution, XSS, Application crashes due to missing input validation of host names returned by Domain Name Servers in Node.js dns library which can lead to output of wrong hostnames (leading to Domain Hijacking) and injection vulnerabilities in applications using the library.
Weakness: Improper Null Termination (CWE-170)
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/AR:L/IR:L/CR:L
CVE-2022-1586
An out-of-bounds read vulnerability was discovered in the PCRE2 library in the compile_xclass_matchingpath() function of the pcre2_jit_compile.c file. This involves a unicode property matching issue in JIT-compiled regular expressions. The issue occurs because the character was not fully read in case-less matching within JIT.
Weakness: Out-of-bounds Read (CWE-125)

Base Score: 9.1
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/AR:L/IR:L/CR:L
CVE-2022-1587
An out-of-bounds read vulnerability was discovered in the PCRE2 library in the get_recurse_data_length() function of the pcre2_jit_compile.c file. This issue affects recursions in JIT-compiled regular expressions caused by duplicate data transfers.
Weakness: Out-of-bounds Read (CWE-125)
Base Score: 9.1
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/AR:L/IR:L/CR:L
CVE-2022-35255
A weak randomness in WebCrypto keygen vulnerability exists in Node.js 18 due to a change with EntropySource() in SecretKeyGenTraits::DoKeyGen() in src/crypto/crypto_keygen.cc. There are two problems with this: 1) It does not check the return value, it assumes EntropySource() always succeeds, but it can (and sometimes will) fail. 2) The random data returned byEntropySource() may not be cryptographically strong and therefore not suitable as keying material.
Weakness: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) (CWE-338)
Base Score: 9.1
Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/AR:L/IR:L/CR:L
CVE-2022-36760
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.
Weakness: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') (CWE-444)
Base Score: 9
Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/AR:L/IR:L/CR:L
CVE-2023-25690
Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.

Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches
some portion of the user-supplied request-target (URL) data and is then
re-inserted into the proxied request-target using variable
substitution. For example, something like:

RewriteEngine on
RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P]
ProxyPassReverse /here/ http://example.com:8080/

Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

Weakness: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') (CWE-444)
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/AR:L/IR:L/CR:L

**General recommendations**

Festo Didactic offers products with security functions that aid the safe operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks from cyber threats, a comprehensive security concept must be implemented and continuously updated. Festo's products and services only constitute one part of such a concept.
The customer is responsible for preventing unauthorized access to their plants, systems, machines and networks. Systems, machines and components should only be connected to a company's network or the Internet if and as necessary, and only when the suitable security measures (e.g., firewalls and network segmentation, defense-in-depth) are in place. Failure to ensure adequate security measures when connecting the product to the network can result in vulnerabilities which allow unauthorized, remote access to the network – even beyond the product's boundaries. This access could be abused to incur a loss of data or manipulate or sabotage systems. Typical forms of attack include but are not limited to: Denial-of-Service (rendering the system temporarily non-functional), remote execution of malicious code, privilege escalation (executing malicious code with higher system privileges than expected), ransomware (encryption of data and demanding payment for decryption). In the context of industrial systems and machines this can also lead to unsafe states, posing a danger to people and equipment.
Furthermore, Festo's guidelines on suitable security measures should be observed. Festo products and solutions are constantly being developed further in order to make them more secure. Festo strongly recommends that customers install product updates as soon as they become available and always use the latest versions of its products. Any use of product versions that are no longer supported or any failure to install the latest updates may render the customer vulnerable to cyber-attacks.

**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-2023-013
- CERT@VDE Security Advisory https://cert.vde.com/en/advisories/vendor/festo
- FactoryViews Upgrade Guide https://ip.festo-didactic.com/InfoportalCMS/a4b1011f0ab575250a2a680c34bd59f6/

**Revision History**

| Version | Date of the revision | Summary of the revision |
|---|---|---|
| 1.0.0 | July 10th, 2023 | Initial version |
| 1.0.1 | January 11th, 2024 | Adjust link to VDE Advisory |

**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.