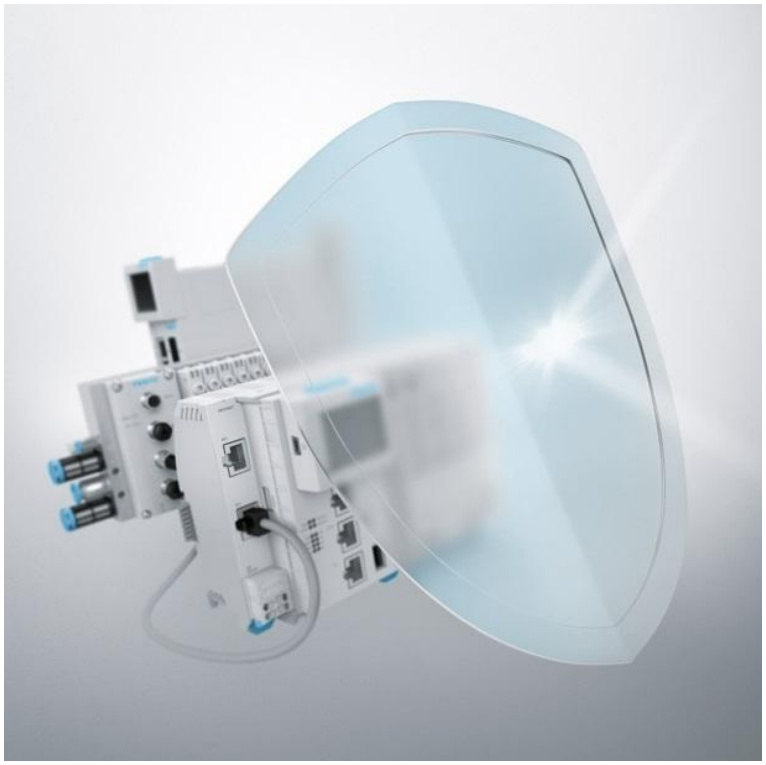
Several Vulnerabilities in MES PC (Windows 10)



FSA-202402

Date
February 27th, 2024

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

MES PCs shipped with Windows 10 come pre-installed with XAMPP. XAMPP is a bundle of third-party open-source applications including the Apache HTTP Server, the MariaDB database and more. From time to time, vulnerabilities in these applications are discovered. These are fixed in newer versions of XAMPP by updating the bundled applications.

MES PCs shipped with Windows 10 include a copy of XAMPP which contains around 140 such vulnerabilities listed in this advisory. They can be fixed by replacing XAMPP with Festo Didactic's Factory Control Panel application.

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 usage of MES PCs for didactic purposes 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.

Vulnerability Identifier

CVEs: CVE-2006-20001, CVE-2013-6501, CVE-2014-9705, CVE-2014-9709, CVE-2015-2301, CVE-2015-2348, CVE-2015-2787, 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-2020-2752, CVE-2020-2760, CVE-2020-2780, CVE-2020-2812, CVE-2020-2814, CVE-2020-2922, 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-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-2021-21702, CVE-2021-21703, CVE-2021-21704, CVE-2021-21705, CVE-2021-21706, CVE-2021-21707, CVE-2021-21708, CVE-2021-27928, CVE-2021-35604, 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-2022-4900, CVE-2022-21595, 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-2022-36760, CVE-2022-37436, CVE-2023-0567, CVE-2023-0568, CVE-2023-0662, 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)

Affected Vendors

Festo Didactic SE

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
MES PC: MES PC shipped with Windows 10 affected		For all CVEs: Festo Didactic has released Factory Control Panel as a replacement for XAMPP on its MES PCs. Contact technical support at services.didactic@festo.com to obtain the current version of Factory Control Panel which includes fixes for these vulnerabilities.

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
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
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
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
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
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
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
CVE-2019-11034
When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash.
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
CVE-2019-11035
When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.28, 7.2.x below 7.2.17 and 7.3.x below 7.3.4 can be caused to read past allocated buffer in exif_iif_add_value function. This may lead to information disclosure or crash.
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
CVE-2019-11036
When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.29, 7.2.x below 7.2.18 and 7.3.x below 7.3.5 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash.
Weakness: Buffer Over-read (CWE-126)
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
CVE-2019-11039
Function iconv_mime_decode_headers() in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 may perform out-of-buffer read due to integer overflow when parsing MIME headers. This may lead to information disclosure or crash.
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
CVE-2019-11040
When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.
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
CVE-2019-11043
In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.

Weakness: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (CWE-120)
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
CVE-2019-11049
In PHP versions 7.3.x below 7.3.13 and 7.4.0 on Windows, when supplying custom headers to mail() function, due to mistake introduced in commit 78f4b4a2dcf92ddbccea1bb95f8390a18ac3342e, if the header is supplied in lowercase, this can result in double-freeing certain memory locations.
Weakness: Double Free (CWE-415)
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
CVE-2020-7059
When using fgetss() function to read data with stripping tags, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause this function to read past the allocated buffer. This may lead to information disclosure or crash.
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
CVE-2020-7060
When using certain mbstring functions to convert multibyte encodings, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause function mbfl_filt_conv_big5_wchar to read past the allocated buffer. This may lead to information disclosure or crash.
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
CVE-2020-7061
In PHP versions 7.3.x below 7.3.15 and 7.4.x below 7.4.3, while extracting PHAR files on Windows using phar extension, certain content inside PHAR file could lead to one-byte read past the allocated buffer. This could potentially lead to information disclosure or crash.
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
CVE-2021-21708
In PHP versions 7.4.x below 7.4.28, 8.0.x below 8.0.16, and 8.1.x below 8.1.3, when using filter functions with FILTER_VALIDATE_FLOAT filter and min/max limits, if the filter fails, there is a possibility to trigger use of allocated memory after free, which can result it crashes, and potentially in overwrite of other memory chunks and RCE. This issue affects: code that uses FILTER_VALIDATE_FLOAT with min/max limits.
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

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
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

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 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-2023-065
- CERT@VDE Security Advisory https://cert.vde.com/en/advisories/vendor/festo

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	February 27th, 2024	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.