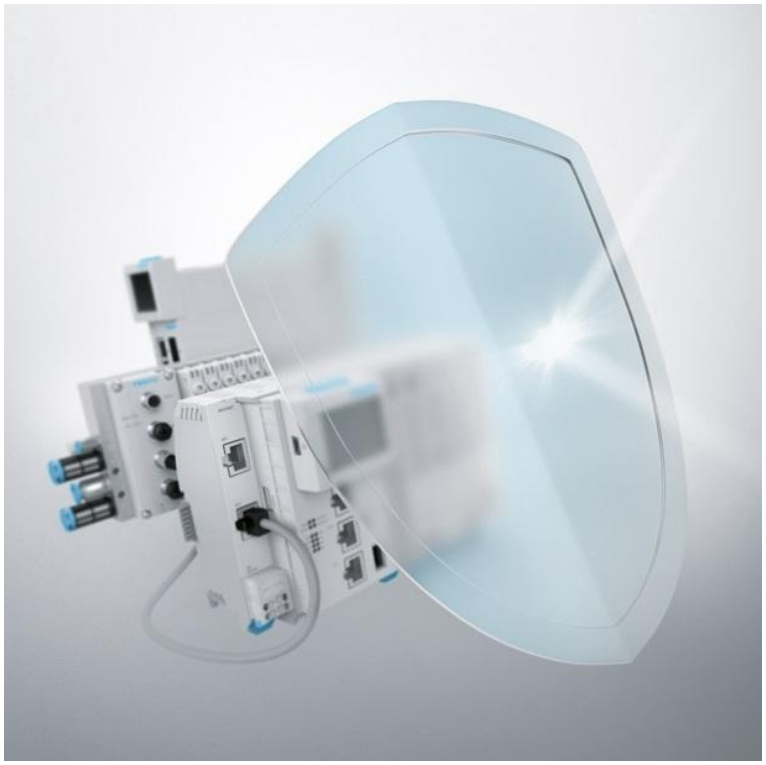
Video.js Cross-Site-Scripting (XSS) vulnerability in LX Appliance



FSA-202301

Date
August 29th, 2023

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 in the Video.js package could allow a user of LX Appliance, with a high privilege account (i.e., with the "Teacher" role), to craft a malicious course and launch an XSS attack.

Vulnerability Identifier

CVEs: CVE-2021-23414

Severity

6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)

Affected Vendors

Festo Didactic SE

Affected Products and Remediations

Affected Product and Versions	Product Details	Remediation
LX Appliance: FESTO LX Appliance (before June 2023) affected	Festo:Partnumber:8167959, 8167960, 8167961, 8167962, 8167963, 8167964	For all CVEs: Contact Festo Didactic services department at services.didactic@festo.com to update your LX Appliance to the latest version.

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-2021-23414
This affects the package video.js before 7.14.3. The src attribute of track tag allows to bypass HTML escaping and execute arbitrary code.
Weakness: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (CWE-79)
Base Score: 6.1

Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

General recommendations

As part of a security strategy, Festo recommends the following general defense measures to reduce the risk of exploits:
- Use LX Appliances only in a protected environment to minimize network exposure and ensure that they are not accessible from outside
- Use firewalls to protect and separate LX Appliances from other networks
- Use VPN (Virtual Private Networks) tunnels if remote access is required
- Limit the access to LX Appliances by physical means, operating system features, etc.

Festo strongly recommends minimizing and protect network access to LX Appliances with state-of-the-art techniques and processes.

Acknowledgments

Festo SE & Co. KG thanks the following parties for their efforts:

- CERT@VDE for Coordination and support for 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-2023-040
- CERT@VDE Security Advisories https://cert.vde.com/en/advisories/vendor/festo/

Revision History

Version	Date of the revision	Summary of the revision
1.0.0	August 28th, 2023	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 of Festo for delivery, payment and software use shall apply, available under http://www.festo.com.