

Forum:[Hack Forums](#)

Thread: [Festo LX Appliance](#)

Stanley - December 17, 2025, 9:05 pm

Festo LX Appliance

View CSAF

1. EXECUTIVE SUMMARY

CVSS v3 6.1

ATTENTION: Exploitable remotely/low attack complexity

Vendor: Festo SE & Co. KG

Equipment: LX Appliance

Vulnerability: Cross-site Scripting

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow a user of LX Appliance with a high privilege account to craft a malicious course and launch an XSS attack.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

Festo reports that the following products are affected:

Festo Software LX Appliance: Versions prior to June 2023

3.2 VULNERABILITY OVERVIEW

3.2.1 IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION

('CROSS-SITE SCRIPTING') CWE-79

The "src" attribute of the "track" tag allows a malicious user to bypass HTML escaping and execute arbitrary code. This affects the package video.js before 7.14.3.

CVE-2021-23414 has been assigned to this vulnerability. A CVSS v3.1 base score of 6.1 has been calculated; the CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).

3.3 BACKGROUND

CRITICAL INFRASTRUCTURE SECTORS: Commercial Facilities, Communications, Critical Manufacturing, Energy

COUNTRIES/AREAS DEPLOYED: Worldwide

COMPANY HEADQUARTERS LOCATION: Germany

3.4 RESEARCHER

Festo coordinated this vulnerability with CERT@VDE.

4. MITIGATIONS

Festo has identified the following specific workarounds and mitigations users can apply to reduce risk:

LX Appliance Versions prior to June 2023: Contact Festo Didactic services department at services.didactic@festo.com to update your LX Appliance to the latest version.

For more information see the associated Festo SE & Co. KG security advisory FSA-202301

FSA-202301: Festo: Cross-Site-Scripting (XSS) vulnerability in LX-Appliance - HTML
FSA-202301: Festo: Cross-Site-Scripting (XSS) vulnerability in LX-Appliance - CSAF.

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability, such as:

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the Internet.

Locate control system networks and remote devices behind firewalls and isolating them from business networks.

When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs). Recognize VPNs may have vulnerabilities, should be updated to the most recent version available, and are only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on [cisa.gov](https://www.cisa.gov). Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at [cisa.gov](https://www.cisa.gov) in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

Do not click web links or open attachments in unsolicited email messages.

Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.

Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

No known public exploitation specifically targeting this vulnerability has been reported to CISA at this time.

5. UPDATE HISTORY

December 09, 2025: Initial Republication of Festo SE & Co. KG FSA-202301

<https://www.cisa.gov/news-events/ics-advisories/icsa-25-343-02>