SSA-268517: Code Execution Vulnerability (libwebp CVE-2023-4863) in Mendix Studio Pro

Publication Date:	2023-11-14
Last Update:	2023-11-14
Current Version:	V1.0
CVSS v3.1 Base Score:	7.5

SUMMARY

Mendix Studio Pro is vulnerable to an out of bounds write vulnerability in the integrated libwebp library (CVE-2023-4863), that could allow an attacker to execute code in the context of a victim user's system.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Mendix Studio Pro 7: All versions < V7.23.37	Update to V7.23.37 or later version https://docs.mendix.com/releasenotes/studio-pro/7/
Mendix Studio Pro 8: All versions < V8.18.27	Update to V8.18.27 or later version https://docs.mendix.com/releasenotes/studio-pro/8/
Mendix Studio Pro 9: All versions < V9.24.0	Update to V9.24.0 or later version https://docs.mendix.com/releasenotes/studio-pro/9/
Mendix Studio Pro 10: All versions < V10.3.1	Update to V10.3.1 or later version https://docs.mendix.com/releasenotes/studio-pro/10/

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

Mendix Studio Pro is a low-code IDE for professional developers. It is a powerful visual model-driven development environment to build apps on the Mendix Platform.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2023-4863

The affected products are vulnerable to an out of bounds write vulnerability in the integrated libwebp library, that could be triggered while parsing specially crafted image files.

This could allow an attacker to execute code in the context of a victim user's system. As a precondition, the user needs to add such image files, or Mendix Marketplace content that contains such image files, to their project. The exploitation happens in certain scenarios when the user opens the document that contains the image.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2023-11-14):	Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.