# SSA-415938: Improper Access Control Vulnerability in Mendix

Publication Date: 2022-03-08
Last Update: 2022-03-08
Current Version: V1.0
CVSS v3.1 Base Score: 7.7

## SUMMARY

A vulnerability in Mendix Studio Pro was discovered, that, if acted upon by a malicious user, could allow to retrieve the status of a job run by another user in certain cases.

Mendix has released updates for the affected product lines, recommends to update to the latest versions and to redeploy the applications.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Mendix Applications using Mendix 7:<br>All versions < V7.23.29 | Update your Mendix Project to V7.23.29 or later version and redeploy your application<br>https://docs.mendix.com/releasenotes/studio-pro/7.23 |

## WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

## 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 is a high productivity app platform that enables you to build and continuously improve mobile and web applications at scale. The Mendix Platform is designed to accelerate enterprise app delivery across your entire application development lifecycle, from ideation to deployment and operations.

## 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-2022-26317

When returning the result of a completed Microflow execution call the affected framework does not correctly verify, if the request was initially made by the user requesting the result. Together with predictable identifiers for Microflow execution calls, this could allow a malicious attacker to retrieve information about arbitrary Microflow execution calls made by users within the affected system.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.7 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-284: Improper Access Control |

## 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 (2022-03-08): Publication Date

## TERMS OF USE