

## **SSA-433782: Improper Access Control Vulnerability in Mendix**

Publication Date: 2022-07-12  
 Last Update: 2022-07-12  
 Current Version: V1.0  
 CVSS v3.1 Base Score: 4.9

### **SUMMARY**

An improper access control vulnerability in Mendix applications was discovered. In case of access to an active user session, the vulnerability could allow to change that user's password by passing password validations within a Mendix application.

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

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
Mendix Applications using Mendix 7: All versions < V7.23.31	Update your Mendix Project to V7.23.31 or later version and redeploy your application <a href="https://docs.mendix.com/releases/notes/studio-pro/7/">https://docs.mendix.com/releases/notes/studio-pro/7/</a>
Mendix Applications using Mendix 8: All versions < V8.18.18	Update your Mendix Project to V8.18.18 or later version and redeploy your application <a href="https://docs.mendix.com/releases/notes/studio-pro/8/">https://docs.mendix.com/releases/notes/studio-pro/8/</a>
Mendix Applications using Mendix 9: All versions < V9.14.0	Update your Mendix Project to V9.14 or later version and redeploy your application <a href="https://docs.mendix.com/releases/notes/studio-pro/9/">https://docs.mendix.com/releases/notes/studio-pro/9/</a>
Mendix Applications using Mendix 9 (V9.6): All versions < V9.6.12	Update your Mendix Project to V9.6.12 or later (preferably to the latest V9.12 version) and redeploy your application <a href="https://docs.mendix.com/releases/notes/studio-pro/9.6/">https://docs.mendix.com/releases/notes/studio-pro/9.6/</a>
Mendix Applications using Mendix 9 (V9.12): All versions < V9.12.2	Update your Mendix Project to V9.12.2 or later version and redeploy your application <a href="https://docs.mendix.com/releases/notes/studio-pro/9.12/">https://docs.mendix.com/releases/notes/studio-pro/9.12/</a>

### **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 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-2022-31257**

In case of access to an active user session in an application that is built with an affected version, it's possible to change that user's password bypassing password validations within a Mendix application. This could allow to set weak passwords.

CVSS v3.1 Base Score      4.9  
CVSS Vector                [CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/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 (2022-07-12):      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](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.