

## **SSA-338732: Information Disclosure Vulnerability in Mendix**

Publication Date: 2021-11-09  
Last Update: 2021-11-09  
Current Version: V1.0  
CVSS v3.1 Base Score: 4.0

### **SUMMARY**

Applications built with affected versions of Mendix Studio Pro do not prevent file documents from being cached when files are opened or downloaded using a browser. This could allow a local attacker to read those documents by exploring the browser cache.

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**

| <b>Affected Product and Versions</b>                           | <b>Remediation</b>   |
|--|--|
| Mendix Applications using Mendix 7:<br>All versions < V7.23.26 | Update to V7.23.26 or later version and redeploy your application<br><a href="https://docs.mendix.com/releases/notes/studio-pro/7">https://docs.mendix.com/releases/notes/studio-pro/7</a><br>See further recommendations from section <a href="#">Workarounds and Mitigations</a>         |
| Mendix Applications using Mendix 8:<br>All versions < V8.18.12 | Update to V8.18.12 or later version and redeploy your application<br><a href="https://docs.mendix.com/releases/notes/studio-pro/8">https://docs.mendix.com/releases/notes/studio-pro/8</a><br>See further recommendations from section <a href="#">Workarounds and Mitigations</a>         |
| Mendix Applications using Mendix 9:<br>All versions < V9.6.1   | Update to V9.6.1 or V9.7.0 or later version and redeploy your application<br><a href="https://docs.mendix.com/releases/notes/studio-pro/9">https://docs.mendix.com/releases/notes/studio-pro/9</a><br>See further recommendations from section <a href="#">Workarounds and Mitigations</a> |

### **WORKAROUNDS AND MITIGATIONS**

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- In applications that were built with affected versions of Mendix Studio Pro: avoid using file documents that contain sensitive information

### **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-2021-42015

Applications built with affected versions of Mendix Studio Pro do not prevent file documents from being cached when files are opened or downloaded using a browser. This could allow a local attacker to read those documents by exploring the browser cache.

|                      |  |
|----------------------|--|
| CVSS v3.1 Base Score | 4.0  |
| CVSS Vector          | <a href="#">CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C</a> |
| CWE                  | CWE-525: Use of Web Browser Cache Containing Sensitive Information         |

## **ACKNOWLEDGMENTS**

Siemens thanks the following parties for their efforts:

- Casix for reporting the vulnerability

## **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 (2021-11-09): 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.