

## **SSA-492173: Expression Injection Vulnerability in Mendix Applications**

Publication Date: 2022-07-12  
Last Update: 2022-07-12  
Current Version: V1.0  
CVSS v3.1 Base Score: 6.5

### **SUMMARY**

An expression injection vulnerability was discovered in the Workflow processing of Mendix Runtime, that can affect the running applications. The vulnerability could allow a malicious user to leak sensitive information if the Workflow visual language of Mendix is used.

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 9:<br>All versions $\geq$ V9.11 < V9.15 | Update to V9.15 or later version<br><a href="https://docs.mendix.com/releases/studio-pro/9/">https://docs.mendix.com/releases/studio-pro/9/</a>         |
| Mendix Applications using Mendix 9 (V9.12):<br>All versions < V9.12.3    | Update to V9.12.3 or later version<br><a href="https://docs.mendix.com/releases/studio-pro/9.12/">https://docs.mendix.com/releases/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-2022-34466**

An expression injection vulnerability was discovered in the Workflow subsystem of Mendix Runtime, that can affect the running applications. The vulnerability could allow a malicious user to leak sensitive information in a certain configuration.

|                      |  |
|----------------------|--|
| CVSS v3.1 Base Score | 6.5  |
| CVSS Vector          | <a href="#">CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C</a>                                 |
| CWE                  | CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') |

## **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.