SSA-210822: Improper Access Control Vulnerability in Mendix Workflow Commons Module

Publication Date: 2022-12-13
Last Update: 2023-01-10
Current Version: V1.1
CVSS v3.1 Base Score: 8.1

SUMMARY

The Mendix Workflow Commons module improperly handles access control for some module entities. This could allow authenticated remote attackers to read or delete sensitive information.

Mendix has released updates for several version lines of the Mendix Workflow Commons module and recommends to update to the latest version.

Note that the fix might slightly impact the module's functionality in specific cases.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Mendix Workflow Commons: All versions < V2.4.0	Update to V2.4.0 or later version https://marketplace.mendix.com/link/component/117066
Mendix Workflow Commons V2.1: All versions < V2.1.4	Update to V2.1.4 or later version https://marketplace.mendix.com/link/component/117066
Mendix Workflow Commons V2.3: All versions < V2.3.2	Update to V2.3.2 or later version https://marketplace.mendix.com/link/component/117066

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 Workflow Commons module provides out-of-the-box content to get you started with building workflows in Mendix.

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-2022-46664

Affected versions of the module improperly handle access control for some module entities.

This could allow authenticated remote attackers to read or delete sensitive information.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

ADDITIONAL INFORMATION

Note that the fix might slightly impact the module's functionality in specific cases.

The Mendix Workflow Commons module provides several version lines to support compatibility with different Mendix framework releases. The fix for CVE-2022-46664 has been backported to support the use of the module for the older Mendix framework versions 9.18 and 9.12.

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 (2022-12-13):	Publication Date
V1.1 (2023-01-10):	Added fix information for older version lines of Mendix Workflow Commons

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.