SSA-779699: Two Incorrect Authorization Vulnerabilities in Mendix

Publication Date: 2021-11-09
Last Update: 2021-11-09
Current Version: V1.0
CVSS v3.1 Base Score: 5.3

SUMMARY

Applications built with affected versions of Mendix Studio Pro do not properly control read or write access for certain client actions. This could allow authenticated attackers to manipulate the content of System.FileDocument objects or to retrieve the changedDate attribute of arbitrary objects.

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 8: All versions < V8.18.13	Update to V8.18.13 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/8 See further recommendations from section Workarounds and Mitigations
Mendix Applications using Mendix 9: All versions < V9.6.2	Update to V9.6.2 or V9.7.0 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/9 See further recommendations from section Workarounds and Mitigations

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-2021-42025

Applications built with affected versions of Mendix Studio Pro do not properly control write access for certain client actions. This could allow authenticated attackers to manipulate the content of System.FileDocument objects in some cases, regardless whether they have write access to it.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-863: Incorrect Authorization

Vulnerability CVE-2021-42026

Applications built with affected versions of Mendix Studio Pro do not properly control read access for certain client actions. This could allow authenticated attackers to retrieve the changedDate attribute of arbitrary objects, even when they don't have read access to them.

CVSS v3.1 Base Score	3.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-863: Incorrect Authorization

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