SSA-875726: Privilege Escalation Vulnerability in Mendix

Publication Date: 2021-04-14
Last Update: 2021-04-14
Current Version: V1.0
CVSS v3.1 Base Score: 8.1

SUMMARY

The latest updates for Mendix fix a vulnerability in Mendix Applications that could allow malicious authorized users to escalate their privileges.

Mendix has released an update for Mendix and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Mendix Applications using Mendix 7: All versions < V7.23.19	Update your Mendix Project to V7.23.19 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/7.23
Mendix Applications using Mendix 8: All versions < V8.17.0	Update your Mendix Project to V8.17.0 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/8.17
Mendix Applications using Mendix 8 (V8.12): All versions < V8.12.5	Update your Mendix Project to V8.12.5 or later and preferably the latest V8.18 version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/8.12
Mendix Applications using Mendix 8 (V8.6): All versions < V8.6.9	Update your Mendix Project to V8.6.9 or later and preferably the latest V8.18 version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/8.6
Mendix Applications using Mendix 9: All versions < V9.0.5	Update your Mendix Project to V9.0.5 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/9.0

WORKAROUNDS AND MITIGATIONS

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

- Remove the privilege to manage user roles for non-administrative roles to mitigate this vulnerability for non-administrative users

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-2021-27394

Authenticated, non-administrative users could modify their privileges by manipulating the user role under certain circumstances, allowing them to gain administrative privileges.

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-269: Improper Privilege Management

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- FlowFabric BV for coordinated disclosure

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 (2021-04-14): Publication Date

TERMS OF USE