SSA-540640: Improper Privilege Management Vulnerability in Mendix Runtime

Publication Date: 2024-06-11
Last Update: 2024-06-11
Current Version: V1.0
CVSS v3.1 Base Score: 5.9
CVSS v4.0 Base Score: 7.4

SUMMARY

Apps built with Mendix Runtime >= V9.3 could allow users with the capability to manage a role to elevate the access rights of users with that role. Successful exploitation requires to guess the id of a target role which contains the elevated access rights.

Siemens has released new versions for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Mendix Applications using Mendix 9: All versions >= V9.3.0 < V9.24.22 affected by CVE-2024-33500	Update to V9.24.22 or later version https://docs.mendix.com/releasenotes/studio-pro/9/ See further recommendations from section Workarounds and Mitigations
Mendix Applications using Mendix 10: All versions < V10.11.0 affected by CVE-2024-33500	Update to V10.11.0 or later version https://docs.mendix.com/releasenotes/studio-pro/10/ See further recommendations from section Workarounds and Mitigations
Mendix Applications using Mendix 10 (V10.6): All versions < V10.6.9 affected by CVE-2024-33500	Update to V10.6.9 or later version https://docs.mendix.com/releasenotes/studio-pro/10/ 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:

- Set the runtime setting ‘StrictReferenceChecks‘ to false; note however, that this comes at the price of making the reference checks less secure

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 DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2024-33500

Affected applications could allow users with the capability to manage a role to elevate the access rights of users with that role. Successful exploitation requires to guess the id of a target role which contains the elevated access rights.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N
CVSS v4.0 Base Score	7.4
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N
CWE	CWE-269: Improper Privilege Management

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Achmea Security Assessment Team 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 (2024-06-11): Publication Date

TERMS OF USE