SSA-084182: Privilege Escalation Vulnerability in Mendix Runtime

Publication Date: 2023-11-14
Last Update: 2023-11-14
Current Version: V1.0
CVSS v3.1 Base Score: 6.8

SUMMARY

Mendix Runtime contains a capture-replay flaw which could have an impact to apps built with the platform, if certain preconditions are met that depend on the app's model and access control design. This could allow authenticated attackers to access or modify objects without proper authorization, or escalate privileges in the context of the vulnerable app.

Siemens has released updates 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 7: All versions < V7.23.37	Update to V7.23.37 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/7/
Mendix Applications using Mendix 8: All versions < V8.18.27	Update to V8.18.27 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/8/
Mendix Applications using Mendix 9: All versions < V9.24.10	Update to V9.24.10 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/9/
Mendix Applications using Mendix 10: All versions < V10.4.0	Update to V10.4.0 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/10/

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-2023-45794

A capture-replay flaw in the platform could have an impact to apps built with the platform, if certain preconditions are met that depend on the app's model and access control design.

This could allow authenticated attackers to access or modify objects without proper authorization, or escalate privileges in the context of the vulnerable app.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-294: Authentication Bypass by Capture-replay

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 (2023-11-14): Publication Date

TERMS OF USE