SSA-870917: Improper Access Control Vulnerability in Mendix

Publication Date: 2022-04-12
Last Update: 2022-04-12
Current Version: V1.0
CVSS v3.1 Base Score: 3.1

SUMMARY

When querying the database, it is possible to sort the results using a protected field. With this an authenticated attacker could extract information about the contents of a protected field.

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 < V7.23.27	Update your Mendix Project to V7.23.27 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/7.23 See further recommendations from section Workarounds and Mitigations
Mendix Applications using Mendix 8: All versions < V8.18.14	Update your Mendix Project to V8.18.14 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/8.18 See further recommendations from section Workarounds and Mitigations
Mendix Applications using Mendix 9: All versions < V9.12.0	Update your Mendix Project to V9.12.0 or later version and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/9.12 See further recommendations from section Workarounds and Mitigations
Mendix Applications using Mendix 9 (V9.6): All versions < V9.6.3	Update your Mendix Project to V9.6.3 or later (preferably to the latest V9.12 version) and redeploy your application https://docs.mendix.com/releasenotes/studio-pro/9.6 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:

- The behavior of sorting by non-accessible attributes can be changed by changing the value of the DataStorage.EnableOrderByEntityAccess custom runtime setting to true. Starting with version 9.12 it is turned on by default with the new, improved behavior.

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-2022-25650

When querying the database, it is possible to sort the results using a protected field. With this an authenticated attacker could extract information about the contents of a protected field.

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-284: Improper Access Control

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 (2022-04-12): Publication Date

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.