

SSA-148641: XPath Constraint Vulnerability in Mendix Runtime

Publication Date: 2022-03-08
Last Update: 2024-10-08
Current Version: V1.3
CVSS v3.1 Base Score: 6.8

SUMMARY

A XPath Constraint vulnerability in the Mendix Runtime was discovered, that can affect the running applications. The vulnerability could allow a malicious user to deduce contents of inaccessible attributes and modify sensitive data.

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 Runtime V7: All versions < V7.23.29 affected by CVE-2022-24309	Update to V7.23.29 or later version https://docs.mendix.com/releases/studio-pro/7/
Mendix Runtime V8: All versions < V8.18.16 affected by CVE-2022-24309	Update to V8.18.16 or later version https://docs.mendix.com/releases/studio-pro/8/
Mendix Runtime V9: All versions < V9.13 only with Runtime Custom Setting *DataStorage.UseNewQueryHandler* set to False affected by CVE-2022-24309	Update to V9.13 or later version For versions < V9.13: Set Runtime Custom Setting <i>DataStorage.UseNewQueryHandler</i> to True or remove the custom setting. The value is set to True by default (see https://docs.mendix.com/developerportal/deploy/environments-details#runtime-tab) https://docs.mendix.com/releases/studio-pro/9/

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 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-2022-24309

If an entity has an association readable by the user, then in some cases, Mendix Runtime may not apply checks for XPath constraints that parse said associations, within apps running on affected versions. A malicious user could use this to dump and manipulate sensitive data.

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-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 (2022-03-08):	Publication Date
V1.1 (2022-04-12):	Summary update; Default configuration for Mendix 9 is not affected; CVSS vector review
V1.2 (2024-05-14):	Added additional fix information for Mendix 9: in versions >= V9.13 the vulnerable configuration is no longer available
V1.3 (2024-10-08):	Renamed affected product from "Mendix Applications using Mendix" to "Mendix Runtime"; fixed a bug in the csaf output

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.