SSA-496604: Cross-Site Scripting Vulnerability in Mendix SAML Module

Publication Date: 2023-01-10
Last Update: 2023-01-10
Current Version: V1.0
CVSS v3.1 Base Score: 9.3

SUMMARY

The Mendix SAML module is affected by a reflected cross-site scripting (XSS) vulnerability that could allow an attacker to extract sensitive information by tricking users into accessing a malicious link. Apps are only vulnerable in certain cases when non-default configuration is used.

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 SAML (Mendix 8 compatible): All versions >= V2.3.0 < V2.3.4	Update to V2.3.4 or later version https://marketplace.mendix.com/link/component/1174/ See further recommendations from section Workarounds and Mitigations
Mendix SAML (Mendix 9 compatible, New Track): All versions >= V3.3.0 < V3.3.9	Update to V3.3.9 or later version https://marketplace.mendix.com/link/component/1174/ See further recommendations from section Workarounds and Mitigations
Mendix SAML (Mendix 9 compatible, Upgrade Track): All versions >= V3.3.0 < V3.3.8	Update to V3.3.8 or later version https://marketplace.mendix.com/link/component/1174/ 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:

- Enable two-factor authentication (2FA), if possible

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 SAML module allows you to use SAML to authenticate your users in your cloud application. This module can communicate with any identity provider that supports SAML2.0 or Shibboleth.

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-2022-46823

The affected module is vulnerable to reflected cross-site scripting (XSS) attacks. This could allow an attacker to extract sensitive information by tricking users into accessing a malicious link.

CVSS v3.1 Base Score	9.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

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 (2023-01-10): 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.