SSA-740594: Privilege Escalation Vulnerability in Mendix SAML Module

Publication Date: 2022-06-14
Last Update: 2022-06-14
Current Version: V1.0
CVSS v3.1 Base Score: 8.3

SUMMARY

The latest updates of Mendix the SAML module fixes two vulnerabilities. One is an XML External Entity (XXE) attack that could allow an attacker to potentially disclose confidential data under certain circumstances the other is an Cross Site Scripting (XSS) attack allowing to execute malicious code by tricking users into accessing a malicious link .

Mendix has released an update for the Mendix SAML module and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Mendix SAML Module (Mendix 7 compatible): All versions < V1.16.6	Update to V1.16.6 or later version https://marketplace.mendix.com/link/component/1174/
Mendix SAML Module (Mendix 8 compatible): All versions < V2.2.2	Update to V2.2.2 or later version https://marketplace.mendix.com/link/component/1174/
Mendix SAML Module (Mendix 9 compatible): All versions < V3.2.3	Update to V3.2.3 or later version https://marketplace.mendix.com/link/component/1174/ For applications upgraded to Mendix 9 from earlier Mendix versions, the issues have already been resolved in V3.2.2

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

The 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-2022-32285

The affected module is vulnerable to XML External Entity (XXE) attacks due to insufficient input sanitation. This may allow an attacker to disclose confidential data under certain circumstances.

CVSS v3.1 Base Score	8.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-611: Improper Restriction of XML External Entity Reference

Vulnerability CVE-2022-32286

In certain configurations SAML module is vulnerable to Cross Site Scripting (XSS) attacks due to insufficient error message sanitation. This could allow an attacker to execute malicious code by tricking users into accessing a malicious link.

CVSS v3.1 Base Score	7.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/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 (2022-06-14): 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.