SSA-522654: Privilege Escalation Vulnerability in Mendix SAML Module

Publication Date: 2021-06-08
Last Update: 2021-06-08
Current Version: V1.0
CVSS v3.1 Base Score: 8.1

SUMMARY

The latest update of Mendix SAML module fixes a privilege escalation vulnerability.

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: All versions < V2.1.2	Update to V2.1.2 or later version https://marketplace.mendix.com/link/component/1174

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific mitigations or workarounds. Please follow General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

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-2021-33712

The configuration of the SAML module does not properly check various restrictions and validations imposed by an identity provider.

This could allow a remote authenticated attacker to escalate privileges.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-345: Insufficient Verification of Data Authenticity

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 (2021-06-08):   Publication Date

TERMS OF USE