

## **SSA-638652 Authentication Bypass Vulnerability in Mendix SAML Module**

Publication Date: 2022-09-13  
Last Update: 2022-09-13  
Current Version: V1.0  
CVSS v3.1 Base Score: 7.4

### **SUMMARY**

The Mendix SAML module insufficiently protects from packet capture replay. This could allow unauthorized remote attackers to bypass authentication and get access to the application.

Mendix has provided fix releases for the Mendix SAML module and recommends to update to the latest version.

Note: For compatibility reasons, fix versions still contain this issue, but only when the not recommended, non default configuration option 'Allow Idp Initiated Authentication' is enabled.

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
Mendix SAML Module (Mendix 7 compatible): All versions < V1.17.0	Update to V1.17.0 or later version <a href="https://marketplace.mendix.com/link/component/1174/">https://marketplace.mendix.com/link/component/1174/</a>
Mendix SAML Module (Mendix 8 compatible): All versions < V2.3.0	Update to V2.3.0 or later version <a href="https://marketplace.mendix.com/link/component/1174/">https://marketplace.mendix.com/link/component/1174/</a>
Mendix SAML Module (Mendix 9 compatible): All versions < V3.3.1	Update to V3.3.1 or later version <a href="https://marketplace.mendix.com/link/component/1174/">https://marketplace.mendix.com/link/component/1174/</a>  For applications upgraded to Mendix 9 from earlier Mendix versions, the issues have already been resolved in V3.3.0

### **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-2022-37011**

Affected versions of the module insufficiently protect from packet capture replay. This could allow unauthorized remote attackers to bypass authentication and get access to the application.

For compatibility reasons, fix versions still contain this issue, but only when the not recommended, non default configuration option 'Allow Idp Initiated Authentication' is enabled.

CVSS v3.1 Base Score	7.4
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C</a>
CWE	CWE-294: Authentication Bypass by Capture-replay

## **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 (2022-09-13): 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](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.