SSA-638652: Authentication Bypass Vulnerability in Mendix SAML Module

Publication Date: 2022-09-13
Last Update: 2022-12-13
Current Version: V1.2
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 are introduced in two release steps:

- The first fix versions address CVE-2022-37011. It removes the vulnerability, except when the not recommended, non default configuration option `'Allow Idp Initiated Authentication'` is enabled.
- The second fix versions address CVE-2022-44457, which removes the issue for the non default configuration as well.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Mendix SAML (Mendix 7 compatible): All versions < V1.17.0	Update to V1.17.0 or later version https://marketplace.mendix.com/link/component/1174/
Mendix SAML (Mendix 7 compatible): All versions >= V1.17.0 < V1.17.2 only affected by CVE-2022-44457	Update to V1.17.2 or later version https://marketplace.mendix.com/link/component/1174/
Mendix SAML (Mendix 8 compatible): All versions < V2.3.0	Update to V2.3.0 or later version https://marketplace.mendix.com/link/component/1174/
Mendix SAML (Mendix 8 compatible): All versions >= V2.3.0 < V2.3.2 only affected by CVE-2022-44457	Update to V2.3.2 or later version https://marketplace.mendix.com/link/component/1174/
Mendix SAML (Mendix 9 compatible, New Track): All versions < V3.3.1	Update to V3.3.1 or later version https://marketplace.mendix.com/link/component/1174/
Mendix SAML (Mendix 9 compatible, New Track): All versions >= V3.3.1 < V3.3.5 only affected by CVE-2022-44457	Update to V3.3.5 or later version https://marketplace.mendix.com/link/component/1174/

Mendix SAML (Mendix 9 compatible, Upgrade Track): All versions < V3.3.0	Update to V3.3.0 or later version https://marketplace.mendix.com/link/component/1174/
Mendix SAML (Mendix 9 compatible, Upgrade Track): All versions >= V3.3.0 < V3.3.4 only affected by CVE-2022-44457	Update to V3.3.4 or later version https://marketplace.mendix.com/link/component/1174/

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 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	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
CWE	CWE-294: Authentication Bypass by Capture-replay

Vulnerability CVE-2022-44457

Affected versions of the module insufficiently protect from packet capture replay, only when the not recommended, non default configuration option `'Allow Idp Initiated Authentication'` is enabled.

This CVE entry describes the incomplete fix for CVE-2022-37011 in a specific non default configuration.

CVSS v3.1 Base Score	7.4
CVSS Vector	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
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
V1.1 (2022-11-08):	Added CVE-2022-44457 and the fix information also for non default configurations
V1.2 (2022-12-13):	Added fix for CVE-2022-44457 for the Mendix 7 compatible version

TERMS OF USE