SSA-851884: Authentication Bypass Vulnerability in Mendix SAML Module

Publication Date: 2023-03-14
Last Update: 2023-08-08
Current Version: V1.2
CVSS v3.1 Base Score: 9.1

SUMMARY

The Mendix SAML module insufficiently verifies the SAML assertions. This could allow unauthenticated 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, fixes for several versions of the Mendix SAML module were introduced in two release steps:

- The first fix versions address CVE-2023-25957. It removes the vulnerability, except when the recommended, default configuration option `'Use Encryption'` is disabled.
- The second fix versions address CVE-2023-29129, 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 >= V1.17.3 < V1.18.0 only affected by CVE-2023-29129	Update to V1.18.0 or later version https://marketplace.mendix.com/link/component/1174
Mendix SAML (Mendix 7 compatible): All versions >= V1.16.4 < V1.17.3	Update to V1.17.3 or later version https://marketplace.mendix.com/link/component/1174
Mendix SAML (Mendix 8 compatible): All versions >= V2.3.0 < V2.4.0 only affected by CVE-2023-29129	Update to V2.4.0 or later version https://marketplace.mendix.com/link/component/1174
Mendix SAML (Mendix 8 compatible): All versions >= V2.2.0 < V2.3.0	Update to V2.3.0 or later version https://marketplace.mendix.com/link/component/1174
Mendix SAML (Mendix 9 latest compatible, New Track): All versions >= V3.3.1 < V3.6.1 only affected by CVE-2023-29129	Update to V3.6.1 or later version https://marketplace.mendix.com/link/component/1174
Mendix SAML (Mendix 9 latest compatible, New Track): All versions >= V3.1.9 < V3.3.1	Update to V3.3.1 or later version https://marketplace.mendix.com/link/component/1174

Mendix SAML (Mendix 9 latest compatible, Upgrade Track): All versions >= V3.3.0 < V3.6.0 only affected by CVE-2023-29129	Update to V3.6.0 or later version https://marketplace.mendix.com/link/component/1174
Mendix SAML (Mendix 9 latest compatible, Upgrade Track): All versions >= V3.1.8 < V3.3.0	Update to V3.3.0 or later version https://marketplace.mendix.com/link/component/1174
Mendix SAML (Mendix 9.6 compatible, New Track): All versions >= V3.1.9 < V3.2.7	Update to V3.2.7 or later version https://marketplace.mendix.com/link/component/1174
Mendix SAML (Mendix 9.6 compatible, Upgrade Track): All versions >= V3.1.8 < V3.2.6	Update to V3.2.6 or later version https://marketplace.mendix.com/link/component/1174
Mendix SAML (Mendix 9.12/9.18 compatible, New Track): All versions >= V3.3.1 < V3.3.15 only affected by CVE-2023-29129	Update to V3.3.15 or later version https://marketplace.mendix.com/link/component/1174
Mendix SAML (Mendix 9.12/9.18 compatible, Upgrade Track): All versions >= V3.3.0 < V3.3.14 only affected by CVE-2023-29129	Update to V3.3.14 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-2023-25957

The affected versions of the module insufficiently verify the SAML assertions. This could allow unauthenticated remote attackers to bypass authentication and get access to the application.

For compatibility reasons, fix versions still contain this issue, but only when the recommended, default configuration option `'Use Encryption'` is disabled.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-303: Incorrect Implementation of Authentication Algorithm

Vulnerability CVE-2023-29129

The affected versions of the module insufficiently verify the SAML assertions. This could allow unauthenticated remote attackers to bypass authentication and get access to the application.

This CVE entry describes the incomplete fix for CVE-2023-25957 in a specific non default configuration.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-303: Incorrect Implementation of Authentication Algorithm

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 (2023-03-14):	Publication Date
V1.1 (2023-06-13):	Added CVE-2023-29129 and the fix information also for non default configurations
V1.2 (2023-08-08):	Added additional release versions of Mendix SAML, where the fixes have been included

TERMS OF USE