SSA-295483: User Enumeration Vulnerability in Mendix Forgot Password Module

Publication Date: 2023-10-10
Last Update: 2023-10-10
Current Version: V1.0
CVSS v3.1 Base Score: 5.3

SUMMARY

The Mendix Forgot Password module contains a user enumeration vulnerability that could allow an attacker to retrieve valid users.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Mendix Forgot Password (Mendix 7 compatible): All versions < V3.7.3	Update to V3.7.3 or later version https://marketplace.mendix.com/link/component/1296
Mendix Forgot Password (Mendix 8 compatible): All versions < V4.1.3	Update to V4.1.3 or later version https://marketplace.mendix.com/link/component/1296
Mendix Forgot Password (Mendix 9 compatible): All versions < V5.4.0	Update to V5.4.0 or later version https://marketplace.mendix.com/link/component/1296
Mendix Forgot Password (Mendix 10 compatible): All versions < V5.4.0	Update to V5.4.0 or later version https://marketplace.mendix.com/link/component/1296

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 Forgot Password module allows your users to sign-up for your application or reset their own password without administrator involvement.

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-2023-43623

Applications using the affected module are vulnerable to user enumeration due to distinguishable responses. This could allow an unauthenticated remote attacker to determine if a user is valid or not, enabling a brute force attack with valid users.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-203: Observable Discrepancy

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 (2023-10-10):	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.