SSA-917115: Mendix Forgot Password Appstore module

Publication Date: 2021-03-09
Last Update: 2021-03-09
Current Version: V1.0
CVSS v3.1 Base Score: 6.8

SUMMARY

Mendix Forgot Password Appstore module contains a vulnerability that could allow authorized users to take over accounts.

Mendix has released an update for the Mendix Forgot Password Appstore module and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Mendix Forgot Password Appstore module: All Versions < V3.2.1	Update to V3.2.1 or later https://marketplace.mendix.com/link/component/1296

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds. Please follow 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

Forgot Password module allow your users to sign-up for your application or reset their own password without administrator involvement. Import this module, assign the roles, the module can generate it's configuration automatically and you are all set to use this component.

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-2021-25672

The Forgot Password Marketplace module does not properly control access. An attacker could take over accounts.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

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 (2021-03-09): Publication Date

TERMS OF USE