SSA-134279: Vulnerability in Mendix Forgot Password Appstore module

Publication Date: 2022-03-08
Last Update: 2022-03-08
Current Version: V1.0
CVSS v3.1 Base Score: 9.1

SUMMARY

Mendix Forgot Password Appstore module contains two vulnerabilities that could allow unauthorized 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 >= V3.3.0 < V3.5.1	Update to V3.5.1 or later https://marketplace.mendix.com/link/component/1296 See further recommendations from section Workarounds and Mitigations
Mendix Forgot Password Appstore module (Mendix 7 compatible): All versions < V3.2.2 only affected by CVE-2022-26314	Update to V3.2.2 or later version https://marketplace.mendix.com/link/component/1296 See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- CVE-2022-26313: Disable sign up as described in the documentation
- Restrict access to application webserver for trusted users only

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-2022-26313

In certain configurations of the affected product, a threat actor could use the sign up flow to hijack arbitrary user accounts.

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-284: Improper Access Control

Vulnerability CVE-2022-26314

Initial passwords are generated in an insecure manner. This could allow an unauthenticated remote attacker to efficiently brute force passwords in specific situations.

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-307: Improper Restriction of Excessive Authentication Attempts

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 (2022-03-08): 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.