SSA-998949: Hard-coded Default Encryption Key in Mendix Encryption Module V10.0.0 and V10.0.1

Publication Date:	2024-07-09
Last Update:	2024-07-09
Current Version:	V1.0
CVSS v3.1 Base Score:	7.5
CVSS v4.0 Base Score:	8.7

SUMMARY

The Mendix Encryption module versions V10.0.0 and V10.0.1 define a specific hard-coded default value for the EncryptionKey constant, which is used in projects where no individual EncryptionKey was specified. This could allow to an attacker to decrypt any encrypted project data, as the default encryption key can be considered compromised.

Siemens has released a new version for Mendix Encryption and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Mendix Encryption: All versions >= V10.0.0 < V10.0.2 affected by CVE-2024-39888	Update to V10.0.2 or later version https://marketplace.mendix.com/link/component/1011

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 Encryption module takes care of the following encryption needs: Plain text encryption (for example, passwords) and FileDocument encryption (for example, files or photos).

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2024-39888

Affected versions of the module define a specific hard-coded default value for the EncryptionKey constant, which is used in projects where no individual EncryptionKey was specified.

This could allow to an attacker to decrypt any encrypted project data, as the default encryption key can be considered compromised.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-547: Use of Hard-coded, Security-relevant Constants

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 (2024-07-09):	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.