SSA-580125: Multiple Vulnerabilities in SIMATIC eaSie

Publication Date: 2022-07-12
Last Update: 2022-08-09
Current Version: V1.1
CVSS v3.1 Base Score: 10.0

SUMMARY

SIMATIC eaSie contains multiple vulnerabilities that could allow an attacker to send arbitrary messages to the underlying message passing framework of the affected system or crash the attached application.

Siemens has released an update for the SIMATIC eaSie Core Package and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC eaSie Core Package (6DL5424-0AX00-0AV8): All versions < V22.00	Update to V22.00 or later version https://support.industry.siemens.com/cs/ww/en/view/109809928

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

SIMATIC eaSie is a digital assistant for automation and process control technology in the Siemens automation concept, "Totally Integrated Automation".

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-2021-44221

The affected systems do not properly validate input that is sent to the underlying message passing framework. This could allow a remote attacker to trigger a denial of service of the affected system.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-44222

The underlying MQTT service of affected systems does not perform authentication in the default configuration. This could allow an unauthenticated remote attacker to send arbitrary messages to the service and thereby issue arbitrary requests in the affected system.

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

ADDITIONAL INFORMATION

These vulnerabilities has been discovered internally by Siemens.

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 (2022-07-12): Publication Date
V1.1 (2022-08-09): Clarified that eaSie Core Package is affected

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.