SSA-587547: Unencrypted Storage of User Credentials in QMS Automotive

Publication Date: 2022-11-08
Last Update: 2022-11-08
Current Version: V1.0
CVSS v3.1 Base Score: 7.6

SUMMARY

QMS Automotive contains a vulnerability that stores user credentials in plantext within the user database. This could allow an attacker to read credentials from memory.

Siemens is preparing updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
QMS Automotive: All versions	Currently no fix is available See 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:

- Enable encryption for user passwords. See user manual under ‘Administration’ for further details

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

Quality Management Systems (QMS) enable manufacturers to electronically monitor, manage and document their quality processes to help ensure that products are manufactured within tolerance, comply with all applicable standards, and do not contain defects. Quality Management System (QMS) software provides the procedures, processes, structure, and resources needed to streamline manufacturing and ERP operations while cost-effectively managing quality issues.

 © Siemens 2022

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-2022-43958

User credentials are stored in plaintext in the database. This could allow an attacker to gain access to credentials and impersonate other users.

CVSS v3.1 Base Score	7.6
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L/E:P/RL:U/RC:C
CWE	CWE-316: Cleartext Storage of Sensitive Information in Memory

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 (2022-11-08): 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.