SSA-147266: Multiple Vulnerabilities in QMS Automotive before V12.39

Publication Date: 2023-09-12
Last Update: 2023-09-12
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

SUMMARY

QMS Automotive before V12.39 contains multiple vulnerabilities that could allow an attacker to perform malicious code injection, information disclosure or lead to a denial of service condition.

Siemens has released an update for QMS Automotive and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
QMS Automotive: All versions < V12.39	Update to V12.39 or later version. The patch is available upon request from customer support

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

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.

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 without any hashing mechanism. 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-256: Plaintext Storage of a Password

Vulnerability CVE-2023-40724

User credentials are found in memory as plaintext. An attacker could perform a memory dump, and get access to credentials, and use it for impersonation.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-316: Cleartext Storage of Sensitive Information in Memory

Vulnerability CVE-2023-40725

The affected application returns inconsistent error messages in response to invalid user credentials during login session. This allows an attacker to enumerate usernames, and identify valid usernames.

CVSS v3.1 Base Score	4.0
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-209: Generation of Error Message Containing Sensitive Information

Vulnerability CVE-2023-40726

The affected application server responds with sensitive information about the server. This could allow an attacker to directly access the database.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-550: Server-generated Error Message Containing Sensitive Information

Vulnerability CVE-2023-40727

The QMS.Mobile module of the affected application uses weak outdated application signing mechanism. This could allow an attacker to tamper the application code.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-347: Improper Verification of Cryptographic Signature

Vulnerability CVE-2023-40728

The QMS.Mobile module of the affected application stores sensitive application data in an external insecure storage. This could allow an attacker to alter content, leading to arbitrary code execution or denial-of-service condition.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-922: Insecure Storage of Sensitive Information

Vulnerability CVE-2023-40729

The affected application lacks security control to prevent unencrypted communication without HTTPS. An attacker who managed to gain machine-in-the-middle position could manipulate, or steal confidential information.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-319: Cleartext Transmission of Sensitive Information

Vulnerability CVE-2023-40730

The QMS.Mobile module of the affected application lacks sufficient authorization checks. This could allow an attacker to access confidential information, perform administrative functions, or lead to a denial-of-service condition.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2023-40731

The affected application allows users to upload arbitrary file types. This could allow an attacker to upload malicious files, that could potentially lead to code tampering.

CVSS v3.1 Base Score	5.7
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-434: Unrestricted Upload of File with Dangerous Type

Vulnerability CVE-2023-40732

The QMS.Mobile module of the affected application does not invalidate the session token on logout. This could allow an attacker to perform session hijacking attacks.

CVSS v3.1 Base Score	3.9
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-613: Insufficient Session Expiration

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 (2023-09-12): Publication Date

TERMS OF USE