SSA-703715: Information Disclosure Vulnerability in Climatix POL909 (AWM)

Publication Date:	2021-11-09
Last Update:	2021-11-09
Current Version:	V1.0
CVSS v3.1 Base Score:	6.4

SUMMARY

Climatix POL909 (AWM module) contains an information disclosure vulnerability could allow an attacker in a man-in-the-middle position to read sensitive data, such as administrator credentials, or modify data in transit.

Siemens has released an update for Climatix POL909 (AWM module) and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Climatix POL909 (AWM module): All versions < V11.34	Update to V11.34 or later version https://support.industry.siemens.com/cs/ww/en/view/109747351

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

The Siemens Climatix AWM (Advanced Web Module, POL909) enables the user of a Climatix 600 solution to implement and load customer Web pages and functions.

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-2021-40366

The web server of affected devices transmits data without TLS encryption. This could allow an unauthenticated remote attacker in a man-in-the-middle position to read sensitive data, such as administrator credentials, or modify data in transit.

CVSS v3.1 Base Score	6.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

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 (2021-11-09):	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.