SSA-252466: Multiple Vulnerabilities in Climatix POL909 (AWM and AWB)

Publication Date: 2022-03-08
Last Update: 2022-03-08
Current Version: V1.0
CVSS v3.1 Base Score: 6.5

SUMMARY

Multiple vulnerabilities have been identified in the Climatix POL909 (AWM and AWB) that could allow an unauthenticated attacker to hijack and redirect users to a malicious webpage, or allow an authenticated attacker to access sensitive files.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Climatix POL909 (AWB module): All versions < V11.44	Update to V11.44 or later version https://support.industry.siemens.com/cs/ww/en/view/109747351/
Climatix POL909 (AWM module): All versions < V11.36	Update to V11.36 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 AWB (Advanced Web and BACnet Module, POL909) enables the user of a Climatix 600 solution to connect to a BACnet IP network and to implement and load customer Web pages and functions.

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-2021-41541

The Group Management page of affected devices is vulnerable to cross-site scripting (XSS). The vulnerability allows an attacker to send malicious JavaScript code which could result in hijacking of the user's cookie/session tokens, redirecting the user to a malicious webpage and performing unintended browser action.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2021-41542

The User Management page of affected devices is vulnerable to cross-site scripting (XSS). The vulnerability allows an attacker to send malicious JavaScript code which could result in hijacking of the user's cookie/session tokens, redirecting the user to a malicious webpage and performing unintended browser action.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2021-41543

The handling of log files in the web application of affected devices contains an information disclosure vulnerability which could allow logged in users to access sensitive files.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

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 (2022-03-08): 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.