SSA-886514: Persistent XSS Vulnerabilities in the Web Interface of Climatix POL908 and POL909 Modules

Publication Date: 2020-04-14
Last Update: 2020-04-14
Current Version: V1.0
CVSS v3.1 Base Score: 6.1

SUMMARY

The Climatix BACnet/IP (POL908) and AWM (POL909) modules contain two persistent cross-site scripting (XSS) vulnerabilities in the web interface that could allow a remote attacker to execute arbitrary JavaScript code in the context of other users' web sessions.

Siemens recommends to update Climatix POL908 and POL909 to the latest version and recommends further countermeasures.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Climatix POL908 (BACnet/IP module): All versions	See recommendations from section Workarounds and Mitigations
Climatix POL909 (AWM module): All versions	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:

- Update Climatix POL908 and POL909 to V11.22 or later version. This update does not solve the XSS issues, but disables the web interface by default, as it is no longer needed in standard use cases.
- Climatix POL908 is designed to be operated in protected BACnet/IP networks only. Do not connect it to other networks, such as an Office LAN or the Internet. Also consider to remove POL908, in case the integrated BACnet/IP implementation in newer versions of Climatix 600 controllers is already sufficient for your environment.

  The remaining mitigation measures apply only, if the web interface if activated (e.g. via the Climatix SCOPE tool):
- Climatix POL909: When configuring your custom web application, disable the access to the default web pages provided by POL909
- Enforce authentication for the web interface, and change the default password of the standard ADMIN user
- Disable JavaScript within the web browser used to access the web server of Climatix POL908
- Utilize a modern web browser with integrated XSS filtering mechanisms

 © Siemens 2020

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 Climatix BACnet/IP communication module (POL908) integrates Climatix 600 controllers into BACnet/IP (BACnet over Internet Protocol) networks.

The 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-2020-7574

A persistent cross-site scripting (XSS) vulnerability exists in the "Server Config" web interface of the affected devices that could allow an attacker to inject arbitrary JavaScript code. The code could be potentially executed later by another (possibly privileged) user.

The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires no system privileges. An attacker could use the vulnerability to compromise the confidentiality and integrity of other users' web session.

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:T/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2020-7575

A persistent cross-site scripting (XSS) vulnerability exists in the web server access log page of the affected devices that could allow an attacker to inject arbitrary JavaScript code via specially crafted GET requests. The code could be potentially executed later by another (privileged) user.

The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires no system privileges. An attacker could use the vulnerability to compromise the confidentiality and integrity of other users' web sessions.

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:T/RC:C
CWE	CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Ezequiel Fernandez from Dreamlab Technologies for reporting the vulnerabilities

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 (2020-04-14): 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.