SSA-142512: Cross-Site Scripting Vulnerability in Climatix BACnet/IP Communication Module

Publication Date 2015-06-25
Last Update 2015-06-25
Current Version V1.0
CVSS Overall Score 3.4

Summary:

The latest version of the Climatix BACnet/IP communication module firmware fixes a vulnerability which could allow cross-site scripting attacks under certain conditions.

AFFECTED PRODUCTS

Climatix BACnet/IP communication module: All versions < V10.34

DESCRIPTION

BACnet/IP communication modules help to integrate controller types POL6XX of the Climatix family into BACnet networks.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://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.

Vulnerability Description (CVE-2015-4174)

The integrated web server (port 80/tcp) of the affected devices could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link.

CVSS Base Score 4.3
CVSS Temporal Score 3.4
CVSS Overall Score 3.4 (AV:N/AC:M/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Mitigating factors

Attackers can only take advantage of the vulnerability if they are able to trick users into accessing a malicious link.

SOLUTION

Siemens provides firmware update Climatix BACnet/IP communication module V10.34 [1] which fixes the vulnerability.

The new firmware update includes further security improvements (e.g. web server authentication enabled by default) and updating to this new release is strongly recommended to all customers. For further information please see the release notes of firmware version V10.34.

As a general security measure Siemens strongly recommends to protect network access to the Climatix BACnet/IP communication module with appropriate mechanisms.

ACKNOWLEDGEMENT

Siemens thanks Juan Francisco Bolivar Hernandez for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

[1] The firmware update for Climatix BACNet Communication Card can be obtained by registered users here:
https://support.industry.siemens.com/cs/ww/en/view/86192510

[2] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
http://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2015-06-25): Publication Date

DISCLAIMER