SSA-632547: Authentication Bypass Vulnerability in SICAM MIC

Publication Date	2015-07-14
Last Update	2015-07-14
Current Version	V1.0
CVSS Overall Score	6.9

Summary:

The latest version of the SICAM MIC firmware fixes a vulnerability which could allow unauthenticated users to perform administrative operations under certain conditions.

AFFECTED PRODUCTS

SICAM MIC: All versions < V2404

DESCRIPTION

The Siemens SICAM MIC is a modular telecontrol device for energy automation that belongs to the SICAM RTUs product family.

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-2015-5386)

Attackers with network access to the device's web interface (port 80/tcp) could possibly circumvent authentication and perform administrative operations. A legitimate user must be logged into the web interface for the attack to be successful.

CVSS Base Score	8.3
CVSS Temporal Score	6.9
CVSS Overall Score	6.9 (AV:N/AC:M/Au:N/C:P/I:P/A:C/E:F/RL:OF/RC:C)

Mitigating factors

For successful exploitation of the vulnerability

- an attacker must have network access to the web interface, and
- a legitimate user must be logged into the web interface

SOLUTION

Siemens provides firmware update V2404 [1] which fixes the vulnerability and contains further security improvements. Siemens recommends customers to update to the latest firmware version.

As a general security measure Siemens strongly recommends to keep the firmware up-to-date and to protect network access to the SICAM MIC with appropriate mechanisms [2]. It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks Philippe Oechslin from Objectif Sécurité for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

[1] The firmware update for SICAM MIC can be obtained here:
http://w3.siemens.com/smartgrid/global/en/products-systems-solutions/substation-automation/remote-terminal-units/Pages/SICAM-MIC.aspx
(Select “Downloads” tab → “Updates and Hotfixes” → “CPC60 mic Central Processing/Communic.”)

[2] Recommended security guidelines for SICAM RTUs are available in the
http://w3.siemens.com/smartgrid/global/en/products-systems-solutions/substation-automation/remote-terminal-units/Pages/SICAM-CMIC.aspx
(Select “Downloads” tab → “Technical Documentation” → “HB Administrator Security Manual”)

[3] 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 (2015-07-14): Publication Date

DISCLAIMER