SSA-452237: Vulnerabilities in Reyrolle

Publication Date 2017-07-04
Last Update 2017-07-04
Current Version V1.0
CVSS v3.0 Base Score 7.5

SUMMARY

The latest firmware update for Reyrolle devices fixes multiple vulnerabilities. The most severe of these vulnerabilities could allow unauthorized users to access the administrative web application.

AFFECTED PRODUCTS

- EN100 Ethernet modules as optional for Reyrolle: All versions < V4.29.01

DESCRIPTION

Reyrolle devices provide a wide range of integrated protection, control, measurement, and automation functions for electrical substations and other fields of application. The Ethernet modules are used for enabling IEC 61850 communication electrical/optical 100 Mbit interfaces for Reyrolle devices.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2016-4784)

The integrated web server (port 80/TCP) of the affected devices could allow remote attackers to obtain sensitive device information if network access was obtained.

CVSS Base Score 5.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability 2 (CVE-2016-4785)

The integrated web server (port 80/ TCP) of the affected devices could allow remote attackers to obtain a limited amount of device memory content if network access was obtained.

CVSS Base Score 5.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability 3 (CVE-2016-7112)

Attackers with network access to the device’s web interface (port 80/ TCP) could possibly circumvent authentication and perform certain administrative operations.

CVSS Base Score 5.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

 © Siemens AG 2017

Vulnerability 4 (CVE-2016-7113)

Specially crafted packets sent to port 80/ TCP could cause the affected device to go into defect mode.

CVSS Base Score 7.5
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

Vulnerability 5 (CVE-2016-7114)

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

CVSS Base Score 4.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Mitigating Factors

The attacker must have network access to the affected devices.

Siemens recommends operating the devices only within trusted networks [2].

SOLUTION

Siemens provides firmware version V4.29.01[1] for EN100 Ethernet module (optional for Reyrolle) fix the vulnerabilities.

As a general security measure Siemens recommends to protect network access with appropriate mechanisms [2] (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] The firmware update for Reyrolle can be obtained from the SIPROTEC 4 downloads area: http://www.siemens.com/downloads/siprotec-4
(expand entry for any SIPROTEC 4 device type supporting IEC 61850 e.g. 7SJ64 → "Firmware and Device Drivers" → "Communication Protocols - IEC 61850" → "Update EN100 V4.29 for all devices over the EN100 interface")

[2] Recommended security guidelines to Secure Substation:
http://www.siemens.com/gridsecurity
(go to "Downloads" side bar →
"Manuals")http://w3.siemens.com/smartgrid/global/en/products-systems-solutions/substation-automation/remote-terminal-units/Pages/SICAM-CMIC.aspx

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

HISTORY DATA

V1.0 (2017-07-04): Publication Date

DISCLAIMER

See: https://www.siemens.com/terms_of_use