SSA-651454: Vulnerabilities in TeleControl Server Basic

Publication Date: 2018-01-25
Last Update: 2018-01-25
Current Version: V1.0
CVSS v3.0 Base Score: 8.8

SUMMARY

The latest update for TeleControl Server Basic resolves three vulnerabilities. One of these vulnerabilities could allow an authenticated attacker with network access to escalate his privileges and perform administrative actions.

Siemens recommends updating to the new version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
TeleControl Server Basic: All versions < V3.1	Install V3.1 https://support.industry.siemens.com/cs/ww/en/view/109755199

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- If TeleControl Server Basic is operated in standalone mode, then customers can close port 8000/tcp on the Windows firewall to mitigate vulnerabilities CVE-2018-4835 and CVE-2018-4836.
- If Telecontrol Server Basic is operated in redundancy mode, then customers can use the Windows firewall to restrict access to port 8000/tcp to the second Telecontrol Server Basics' IP address to mitigate vulnerabilities CVE-2018-4835 and CVE-2018-4836.
- Customers can use the Windows firewall to close port 80/tcp and 443/tcp to mitigate vulnerability CVE-2018-4837.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to run the devices in a protected IT environment, Siemens particularly recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

TeleControl Server Basic allows remote monitoring and control of plants.

VULNERABILITY CLASSIFICATION

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

Vulnerability (CVE-2018-4835)

An attacker with network access to the TeleControl Server Basic's port 8000/tcp could bypass the authentication mechanism and read limited information.

CVSS v3.0 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 (CVE-2018-4836)

An authenticated attacker with a low-privileged account to the TeleControl Server Basic's port 8000/tcp could escalate his privileges and perform administrative operations.

CVSS v3.0 Base Score	8.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability (CVE-2018-4837)

An attacker with access to the TeleControl Server Basic's webserver (port 80/tcp or 443/tcp) could cause a Denial-of-Service condition on the web server. The remaining functionality of the TeleControl Server Basic is not affected by the Denial-of-Service condition.

CVSS v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

ADDITIONAL INFORMATION

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 (2018-01-25): 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.