SSA-126840: Vulnerability in Communication Processor module CP 44x-1 RNA

Publication Date 2017-06-20
Last Update 2017-06-20
Current Version V1.0
CVSS v3.0 Base Score 9.8

SUMMARY

Siemens has released update V1.4.1 for SIMATIC CP 44x-1 RNA modules that resolves a vulnerability that could allow unauthenticated users to perform administrative actions under certain conditions. Siemens recommends specific countermeasures until fixes can be applied.

AFFECTED PRODUCTS

- SIMATIC CP 44x-1 RNA: All versions < V1.4.1

DESCRIPTION

The Communication Processor (CP) of the Redundant Network Access (RNA) series have been designed to connect SIMATIC S7-400 CPUs to Industrial Ethernet.

Detailed information about the vulnerability 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 (CVE-2017-6868)

An unauthenticated remote user could perform administrative actions on the affected Communication Processor (CP) if network access (port 102/TCP) is available, and the CP's configuration is stored on the corresponding CPU.

CVSS Base Score 9.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Mitigating Factors

The attacker must have network access to port 102/TCP of the affected device and the configuration data of the CP must be stored on the CPU.

SOLUTION

Siemens provides a firmware update V1.4.1 [1] for SIMATIC CP 44x-1 RNA modules which fixes the vulnerability and recommends customers update to the fixed version.

Siemens recommends the following mitigations until patches can be applied:

- Apply cell protection concept [2]
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth [3]

As a general security measure, Siemens strongly recommends configuring the environment according to our operational guidelines [2].

ADDITIONAL RESOURCES

[1] Firmware update V1.4.1 for SIMATIC CP 44x-1 RNA module can be obtained at:
https://support.industry.siemens.com/cs/ww/en/view/109748227

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[3] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[4] 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 (2017-06-20): Publication Date

DISCLAIMER