SSA-833048: Vulnerability in SIMATIC S7-1200 CPUs prior to V4

Publication Date 2016-03-14
Last Update 2016-03-14
Current Version V1.0
CVSSv2 Overall Score 5.0

SUMMARY

Siemens became aware that the discontinued products SIMATIC S7-1200 CPUs prior to version 4 could allow for the circumvention of user program block protection under certain conditions.

AFFECTED PRODUCTS

SIMATIC S7-1200 CPU family: All versions < V4.0

DESCRIPTION

Products of the Siemens SIMATIC S7-1200 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 2 (CVSSv2) (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-2016-2846)

SIMATIC S7-1200 CPU prior to version 4 could possibly allow an attacker to circumvent user program block protection under certain circumstances.

Base Score	6.5
Temporal Score	5.0
Overall Score	5.0 (AV:N/AC:L/Au:N/C:P/I:P/A:N/E:POC/RL:OF/RC:C)

Mitigating Factors

The attacker must have network access to an affected device, and the PLC’s access protection must be disabled.

Siemens recommends operating the devices only within trusted networks [3], and recommends enabling the PLC functionality access protection.

SOLUTION

Siemens provides the SIMATIC S7-1200 CPU product release V4.0 or later [1] which fixes this vulnerability. Siemens recommends to keep the firmware up-to-date and to set the PLC functionality “Access protection” to read/write protection.

As a general security measure Siemens strongly recommends to protect network access to S7-1200 CPUs with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks Maik Brüggemann and Ralf Spenneberg from Open Source Training for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

[1] Siemens product release V4.1 firmware requires the use of S7-1200 V4.0 CPU hardware. Further details on the S7-1200 V4.1 release can be found here: http://support.automation.siemens.com/WW/view/en/106200276

[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 (2016-03-14): Publication Date

DISCLAIMER