SSA-750824: Denial-of-Service Vulnerability in Profinet Devices

Publication Date: 2020-02-11
Last Update: 2020-03-10
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

SIMATIC S7-1500 CPU family devices are affected by a vulnerability that could allow an attacker to perform a Denial-of-Service attack if specially crafted UDP packets are sent to the device.

Siemens has released updates for the affected products and recommends that customers update to these new versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions >= V2.5 and < V20.8	Update to V20.8 (V2x.8 corresponds to V2.8 of the S7-1500 CPU firmware) https://support.industry.siemens.com/cs/ww/en/view/109759122
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions >= V2.5 and < V2.8	Update to V2.8 https://support.industry.siemens.com/cs/ww/en/view/109773807
SIMATIC S7-1500 Software Controller: All versions >= V2.5 and < V20.8	Update to V20.8 (V2x.8 corresponds to V2.8 of the S7-1500 CPU firmware) https://support.industry.siemens.com/cs/de/en/view/109772864

WORKAROUNDS AND MITIGATIONS

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

- Restrict network access to affected devices.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens 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

Products of the SIMATIC S7-1500 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

The SIMATIC ET 200SP Open Controller is a PC-based version of the SIMATIC S7-1500 Controller including optional visualization in combination with central I/Os in a compact device.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2019-19281

Affected devices contain a vulnerability that allows an unauthenticated attacker to trigger a Denial-of-Service condition. The vulnerability can be triggered if specially crafted UDP packets are sent to the device.

The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the device availability.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2020-02-11): Publication Date
V1.1 (2020-03-10): Added update for SIMATIC ET 200SP Open Controller CPU 1515SP PC2

TERMS OF USE