SSA-593272: SegmentSmack in Interniche IP-Stack based Industrial Devices

Publication Date: 2020-04-14
Last Update: 2020-05-12
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

A vulnerability exists in affected products that could allow remote attackers to affect the availability of the devices under certain conditions.

The underlying TCP stack can be forced to make very computation expensive calls for every incoming packet which can lead to a Denial-of-Service.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
KTK ATE530S: All versions	See recommendations from section Workarounds and Mitigations
SIDOOR ATD430W: All versions	See recommendations from section Workarounds and Mitigations
SIDOOR ATE530S COATED: All versions	See recommendations from section Workarounds and Mitigations
SIDOOR ATE531S: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants): All versions < V2.0	Update to V2.1.7 https://support.industry.siemens.com/cs/ww/en/view/109759122/
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V2.0	Update to V20.8 https://support.industry.siemens.com/cs/ww/en/view/109759122/
SIMATIC ET200MP IM155-5 PN HF (incl. SIPLUS variants): All versions >= V4.2	See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 MF HF: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN HA (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations

SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants): All versions >= V4.2	See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN/2 HF (incl. SIPLUS variants): All versions >= V4.2	See recommendations from section Workarounds and Mitigations
SIMATIC ET200SP IM155-6 PN/3 HF (incl. SIPLUS variants): All versions >= V4.2	See recommendations from section Workarounds and Mitigations
SIMATIC MICRO-DRIVE PDC: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC PN/PN Coupler (incl. SIPLUS NET variants): All versions >= V4.2	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.0	Update to V2.8 if possible https://support.industry.siemens.com/cs/ww/en/view/109773807/
SIMATIC S7-1500 Software Controller: All versions < V2.0	Update to V20.8 https://support.industry.siemens.com/cs/ww/en/view/109772864/
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 H V6 CPU family and below (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP V7 and below CPU family (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-410 CPU family (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC TDC CP51M1: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC TDC CPU555: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC WinAC RTX (F) 2010: All versions	See recommendations from section Workarounds and Mitigations
SINAMICS S/G Control Unit w. PROFINET: All versions	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds. Please follow General Security Recommendations.

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

SIDOOR is an automatic door management system that offers diverse application options and benefits in elevator, industrial and railway applications.

SIMATIC ET 200 Interface modules for PROFINET IO are used to connect field devices (IO Devices) to controllers (IO Controller) via PROFINET.

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.

SIMATIC MICRO-DRIVE PDC are drive converters for servo drives in the protective extra low voltage range.

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.

Products of the Siemens SIMATIC S7-300 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

Products in the SIMATIC S7-400 CPU family have been designed for process control in industrial environments. They are used worldwide, e.g. in the automotive industry, mechanical equipment manufacture, warehousing systems, building engineering, steel industry, power generation and distribution, pharmaceuticals, food and beverages industry, or chemical industry.

SIMATIC TDC is a multiprocessor automation system for drive, control and technology tasks. The system is used particularly for large plants.

SIMATIC WinAC RTX (F) 2010 is a SIMATIC software controller for PC-based automation solutions.

The SINAMICS converter family is used to control a wide variety of drives, especially in mechanical engineering and plant construction.

PN/PN coupler is used for connecting two PROFINET networks.

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-2019-19300

The Interniche-based TCP Stack can be forced to make very expensive calls for every incoming packet which can lead to a denial of service.

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:U/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

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 (2020-04-14):	Publication Date
V1.1 (2020-05-12):	Added SIMATIC S7-400 H V6 CPU family and below to the list of affected products

TERMS OF USE