SSA-594364: Denial-of-Service Vulnerability in SNMP Implementation of WinCC Runtime

Publication Date: 2021-05-11
Last Update: 2021-05-11
Current Version: V1.0
CVSS v3.1 Base Score: 5.3

SUMMARY

A denial-of-service vulnerability in WinCC Runtime could allow an unauthenticated attacker with network access to cause a denial-of-service condition in the SNMP service by sending crafted SNMP packets to port 161/udp.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC HMI Comfort Panels 1st Generation (incl. SIPLUS variants): All versions < V16 Update 4	Update to V16 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109775861/
SIMATIC HMI KTP Mobile Panels: All versions < V16 Update 4	Update to V16 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109775861/

WORKAROUNDS AND MITIGATIONS

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

- Disable SNMP if this is supported by the product. Disabling SNMP fully mitigates the vulnerability
- Restrict network access to port 161/udp of affected devices to trusted devices or IP addresses

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

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

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-2019-19276

Specially crafted packets sent to port 161/udp can cause the SNMP service of affected devices to crash. A manual restart of the device is required to resume operation of the service.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Younes Dragoni and Alessandro Di Pinto from Nozomi Networks for coordinated disclosure

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 (2021-05-11): Publication Date

TERMS OF USE