

SSA-834884: Vulnerability in SINETPLAN

Publication Date: 2019-09-10
Last Update: 2019-09-10
Current Version: V1.0
CVSS v3.0 Base Score: 8.0

SUMMARY

A vulnerability has been identified in SINETPLAN that could allow local users to execute arbitrary application commands without proper authentication.

Siemens provides a solution that fixes the vulnerability and recommends that users apply the update.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINETPLAN: V2.0	Install TIA Administrator V1.0 SP1 Upd1 https://support.industry.siemens.com/cs/ww/en/view/114358

WORKAROUNDS AND MITIGATIONS

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

- Restrict access to port 8888/tcp to localhost

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

The Siemens Network Planner (SINETPLAN) supports you as a planner of automation systems based on PROFINET. It facilitates the professional planning, calculation, and simulation of load in a PROFINET network and supports virtual commissioning of the network. SINETPLAN provides the capability to efficiently plan and layout PROFINET networks. It supports both "non-real-time communication", such as when TCP/IP data is used, as well as real-time (RT) or IRT communication.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (<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.

Vulnerability CVE-2019-10915

The integrated configuration web application allows to execute certain application commands without proper authentication.

The vulnerability could be exploited by an attacker with local access to the affected system. Successful exploitation requires no privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality and integrity and availability of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	8.0
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C

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 (2019-09-10): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.