SSA-721298: Missing Authentication Vulnerability in TIA Administrator (TIA Portal)

Publication Date: 2019-07-09
Last Update: 2019-07-09
Current Version: V1.0
CVSS v3.0 Base Score: 8.0

SUMMARY

The latest update for TIA Administrator (TIA Portal) fixes a vulnerability that could allow local users to execute arbitrary application commands without proper authentication.

Siemens has released an update for the affected software and provides workarounds and mitigations until the update can be applied.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
TIA Administrator: All versions < V1.0 SP1 Upd1	Update to 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 (default)

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 WinCC (TIA Portal) is an engineering software to configure and program SIMATIC Panels, SIMATIC Industrial PCs, and Standard PCs running WinCC Runtime Advanced or SCADA System WinCC Runtime Professional visualization software.

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 (TIA Administrator) 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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Joseph Bingham from Tenable 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 (2019-07-09): Publication Date

TERMS OF USE