SSA-629512: Local Privilege Escalation Vulnerability in TIA Portal

Publication Date: 2020-01-14
Last Update: 2021-01-12
Current Version: V1.2
CVSS v3.1 Base Score: 7.8

SUMMARY

The latest updates for TIA Portal fix a vulnerability that could allow a local attacker to execute arbitrary code with SYSTEM privileges.

Siemens has released updates for the affected products and recommends to update to the latest version(s).

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
TIA Portal V14: All versions < V14 SP1 Update 10	Update to V14 SP1 Update 10 or later version https://support.industry.siemens.com/cs/us/en/view/109747387/
TIA Portal V15: All versions < V15 SP1 Update 4	Update to V15 SP1 Update 4 or later version https://support.industry.siemens.com/cs/us/en/view/109763890/
TIA Portal V16: All versions < V16 Update 1	Update to V16 Update 1 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:

- Remove write permissions for every non-administrative user on files and folders located below the “TraceEngine” folder (usually located at “C:\ProgramData\Siemens\Automation”).

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 Totally Integrated Automation Portal (TIA Portal) is a PC software that provides access to the complete range of Siemens digitalized automation services, from digital planning and integrated engineering to transparent operation.

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-2019-10934

Changing the contents of a configuration file could allow an attacker to execute arbitrary code with SYSTEM privileges.

The security vulnerability could be exploited by an attacker with a valid account and limited access rights on the system. No user interaction is required.

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

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Wiliam Knowles from Applied Risk for reporting the vulnerability

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 (2020-01-14): Publication Date
V1.1 (2020-04-14): Added solution for TIA Portal V16
V1.2 (2021-01-12): Added solution for TIA Portal V14

TERMS OF USE