SSA-979106: Vulnerabilities in SIMATIC STEP 7 (TIA Portal) and SIMATIC WinCC (TIA Portal)

Publication Date:	2018-08-07
Last Update:	2018-10-09
Current Version:	V1.1
CVSS v3.0 Base Score:	8.6

SUMMARY

The latest updates for SIMATIC STEP 7 (TIA Portal) and SIMATIC WinCC (TIA Portal) fix two vulnerabilities. These two vulnerabilities could either allow an attacker with local file write access to manipulate files and cause a Denial-of-service-condition, or execute code both on the manipulated installation and on devices that are configured using the manipulated installation.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC STEP 7 (TIA Portal) and WinCC (TIA Portal) V10, V11, V12: All versions	Upgrade to V13 SP2 Update 2 https://support.industry.siemens.com/cs/ww/en/view/109759753
SIMATIC STEP 7 (TIA Portal) and WinCC (TIA Portal) V13: All versions < V13 SP2 Update 2	Update to V13 SP2 Update 2 https://support.industry.siemens.com/cs/ww/en/view/109759753
SIMATIC STEP 7 (TIA Portal) and WinCC (TIA Portal) V14: All versions < V14 SP1 Update 6	Update to V14 SP1 Update 6 https://support.industry.siemens.com/cs/ww/en/view/109747387
SIMATIC STEP 7 (TIA Portal) and WinCC (TIA Portal) V15: All versions < V15 Update 2	Update to V15 Update 2 or newer https://support.industry.siemens.com/cs/ww/en/view/109755826

WORKAROUNDS AND MITIGATIONS

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

- Restrict operating system access to authorized personnel.
- Validate GSD files for legitimacy and process GSD files only from trusted sources.

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 unrestricted 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 3.0 (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-2018-11453

Improper file permissions in the default installation of TIA Portal may allow an attacker with local file system access to insert specially crafted files which may prevent TIA Portal startup (Denial-of-Service) or lead to local code execution. No special privileges are required, but the victim needs to attempt to start TIA Portal after the manipulation.

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

CVSS v3.0 Base Score	7.8
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-11454

Improper file permissions in the default installation of TIA Portal may allow an attacker with local file system access to manipulate ressources which may be transferred to devices and executed there by a different user. No special privileges are required, but the victim needs to transfer the manipulated files to a device. Execution is caused on the target device rather than on the PG device.

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

CVSS v3.0 Base Score	8.6
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Younes Dragoni from Nozomi Networks for coordinated disclosure
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for coordination efforts

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 (2018-08-07):	Publication Date
V1.1 (2018-10-09):	Added update for SIMATIC STEP 7 (TIA Portal) and WinCC (TIA Portal) V13

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.