SSA-825651: Deserialization Vulnerability in SIMATIC STEP 7 (TIA Portal) before V18 Update 2

Publication Date: 2024-07-09
Last Update: 2024-07-09
Current Version: V1.0
CVSS v3.1 Base Score: 7.8
CVSS v4.0 Base Score: 8.5

SUMMARY

Affected applications do not properly restrict the .NET BinaryFormatter when deserializing user-controllable input. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application.

Siemens has released a new version for SIMATIC STEP 7 (TIA Portal) V18 and recommends to update to the latest version. Siemens recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC PCS neo V4.0: All versions affected by CVE-2022-45147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal):	See below See recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V16:	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 V16: All versions affected by CVE-2022-45147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V17:	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 V17: All versions affected by CVE-2022-45147	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V18:	Update to V18 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817218/ See further recommendations from section Workarounds and Mitigations

SIMATIC STEP 7 V18: All versions < V18 Update 2 affected by CVE-2022-45147	Update to V18 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817218/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Avoid opening untrusted files from unknown sources in affected products

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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 PCS neo is a distributed control system (DCS).

SIMATIC STEP 7 (TIA Portal) is an engineering software to configure and program SIMATIC controllers.

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 DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2022-45147

Affected applications do not properly restrict the .NET BinaryFormatter when deserializing user-controllable input. This could allow an attacker to cause a type confusion and execute arbitrary code within the affected application.

This is the same issue that exists for .NET BinaryFormatter https://docs.microsoft.com/en-us/visualstudio/code-quality/ca2300.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	8.5
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-502: Deserialization of Untrusted Data

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 (2024-07-09):	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.