SSA-779936: Catalog-Profile Deserialization Vulnerability in Siemens Engineering Platforms before V19

Publication Date: 2024-07-09
Last Update: 2024-07-09
Current Version: V1.0
CVSS v3.1 Base Score: 6.5
CVSS v4.0 Base Score: 7.0

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 new versions for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Totally Integrated Automation Portal (TIA Portal):	See below See further recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V16:	See below See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 Safety V16: All versions < V16 Update 7 affected by CVE-2023-32735	Update to V16 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109772968/ See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 V16: All versions < V16 Update 7 affected by CVE-2023-32735	Update to V16 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109771628/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Unified V16: All versions < V16 Update 7 affected by CVE-2023-32735	Update to V16 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109771777/ See further recommendations from section Workarounds and Mitigations

SIMATIC WinCC V16: All versions < V16.7 affected by CVE-2023-32735	Update to V16.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109775861/ See further recommendations from section Workarounds and Mitigations
SIMOCODE ES V16: All versions < V16 Update 7 affected by CVE-2023-32735	Update to V16 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109771671/ See further recommendations from section Workarounds and Mitigations
SIMOTION SCOUT TIA V5.4 SP1: All versions affected by CVE-2023-32735	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SINAMICS Startdrive V16: All versions affected by CVE-2023-32735	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Soft Starter ES V16: All versions < V16 Update 7 affected by CVE-2023-32735	Update to V16 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109771656/ See further recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V17:	See below See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 Safety V17: All versions < V17 Update 7 affected by CVE-2023-32735	Update to V17 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109784441/ See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 V17: All versions < V17 Update 7 affected by CVE-2023-32735	Update to V17 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109784441/ See further recommendations from section Workarounds and Mitigations
SIMATIC WinCC Unified V17: All versions < V17 Update 7 affected by CVE-2023-32735	Update to V17 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109784441/ See further recommendations from section Workarounds and Mitigations

SIMATIC WinCC V17: All versions < V17.7 affected by CVE-2023-32735	Update to V17.7 or later version https://support.industry.siemens.com/cs/ww/en/view/109784441/ See further recommendations from section Workarounds and Mitigations
SIMOCODE ES V17: All versions < V17 Update 7 affected by CVE-2023-32735	Update to V17 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109803780/ See further recommendations from section Workarounds and Mitigations
SIMOTION SCOUT TIA V5.4 SP3: All versions affected by CVE-2023-32735	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SINAMICS Startdrive V17: All versions affected by CVE-2023-32735	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIRIUS Safety ES V17: All versions < V17 Update 7 affected by CVE-2023-32735	Update to V17 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109793090/ See further recommendations from section Workarounds and Mitigations
SIRIUS Soft Starter ES V17: All versions < V17 Update 7 affected by CVE-2023-32735	Update to V17 Update 7 or later version https://support.industry.siemens.com/cs/ww/en/view/109803801/ See further recommendations from section Workarounds and Mitigations
Totally Integrated Automation Portal (TIA Portal) V18:	See below See further recommendations from section Workarounds and Mitigations
SIMATIC STEP 7 Safety V18: All versions < V18 Update 2 affected by CVE-2023-32735	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-2023-32735	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 WinCC Unified V18: All versions < V18 Update 2 affected by CVE-2023-32735	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 WinCC V18: All versions < V18 Update 2 affected by CVE-2023-32735	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
SIMOCODE ES V18: All versions < V18 Update 2 affected by CVE-2023-32735	Update to V18 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109815534/ See further recommendations from section Workarounds and Mitigations
SIMOTION SCOUT TIA V5.5 SP1: All versions affected by CVE-2023-32735	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SINAMICS Startdrive V18: All versions affected by CVE-2023-32735	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIRIUS Safety ES V18: All versions < V18 Update 2 affected by CVE-2023-32735	Update to V18 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817575/ See further recommendations from section Workarounds and Mitigations
SIRIUS Soft Starter ES V18: All versions < V18 Update 2 affected by CVE-2023-32735	Update to V18 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817573/ See further recommendations from section Workarounds and Mitigations
TIA Portal Cloud V3.0: All versions < V18 Update 2 affected by CVE-2023-32735	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 STEP 7 (TIA Portal) is an engineering software to configure and program SIMATIC controllers.

SIMATIC STEP 7 Safety Basic / Advanced is the high-performance add-on package for programming of fail-safe S7 controllers for the Totally Integrated Automation Portal

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system.

SIMOCODE ES is the central software package for the configuration, commissioning, operation, and diagnosis of SIMOCODE pro. The software is based on the Totally Integrated Automation Portal (TIA Portal) central engineering framework and can be seamlessly integrated if additional TIA Portal-based software such as STEP 7 and WinCC is present.

Soft Starter ES is the central software for configuration, commissioning, operation and diagnostics of the SIRIUS 3RW55, 3RW52 and 3RW44 soft starters.

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-2023-32735

Affected applications do not properly restrict the .NET BinaryFormatter when deserializing hardware configuration profiles. 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	6.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	7.0
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/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