SSA-962515: Out of Bounds Read Vulnerability in Industrial Products

Publication Date: 2024-05-14
Last Update: 2024-07-09
Current Version: V1.1
CVSS v3.1 Base Score: 6.5
CVSS v4.0 Base Score: 8.2

SUMMARY

Several industrial products contain an out of bounds read vulnerability that could allow an attacker to cause a Blue Screen of Death (BSOD) crash of the underlying Windows kernel, leading to denial of service condition.

Siemens has released new versions for several affected products and recommends to update to the latest versions. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
S7-PCT: All versions affected by CVE-2023-46280	Currently no fix is available
Security Configuration Tool (SCT): All versions affected by CVE-2023-46280	Currently no fix is planned
SIMATIC Automation Tool: All versions affected by CVE-2023-46280	Currently no fix is available
SIMATIC BATCH V9.1: All versions affected by CVE-2023-46280	Currently no fix is available
SIMATIC NET PC Software:	See below
SIMATIC NET PC Software V16: All versions affected by CVE-2023-46280	Currently no fix is available
SIMATIC NET PC Software V17: All versions affected by CVE-2023-46280	Currently no fix is available
SIMATIC NET PC Software V18: All versions < V18 SP1 affected by CVE-2023-46280	Update to V18 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109972655/
SIMATIC PCS 7 V9.1: All versions affected by CVE-2023-46280	Currently no fix is available
SIMATIC PDM V9.2: All versions affected by CVE-2023-46280	Currently no fix is available

SIMATIC Route Control V9.1: All versions affected by CVE-2023-46280	Currently no fix is available
SIMATIC STEP 7 V5: All versions affected by CVE-2023-46280	Currently no fix is available
SIMATIC WinCC OA V3.17: All versions affected by CVE-2023-46280	Currently no fix is planned
SIMATIC WinCC OA V3.18: All versions < V3.18 P025 affected by CVE-2023-46280	Update to V3.18 P025 or later version https://www.winccoa.com/downloads/category/versions-patches.html
SIMATIC WinCC OA V3.19: All versions < V3.19 P010 affected by CVE-2023-46280	Update to V3.19 P010 or later version https://www.winccoa.com/downloads/category/versions-patches.html
SIMATIC WinCC Runtime Advanced: All versions affected by CVE-2023-46280	Currently no fix is available
SIMATIC WinCC Runtime Professional V16: All versions < V16 Update 6 affected by CVE-2023-46280	Update to V16 Update 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109776017/
SIMATIC WinCC Runtime Professional V17: All versions affected by CVE-2023-46280	Currently no fix is available
SIMATIC WinCC Runtime Professional V18: All versions < V18 Update 4 affected by CVE-2023-46280	Update to V18 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109807225/
SIMATIC WinCC Runtime Professional V19: All versions < V19 Update 2 affected by CVE-2023-46280	Update to V19 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109820999/
SIMATIC WinCC V7.4: All versions affected by CVE-2023-46280	Currently no fix is planned
SIMATIC WinCC V7.5: All versions < V7.5 SP2 Update 17 affected by CVE-2023-46280	Update to V7.5 SP2 Update 17 or later version https://support.industry.siemens.com/cs/ww/en/view/109793460/
SIMATIC WinCC V8.0: All versions < V8.0 Update 5 affected by CVE-2023-46280	Update to V8.0 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109818723/
SINAMICS Startdrive: All versions < V19 SP1 affected by CVE-2023-46280	Update to V19 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109963196/

SINUMERIK ONE virtual: All versions < V6.23 affected by CVE-2023-46280	Update to V6.23 or later version
SINUMERIK PLC Programming Tool: All versions affected by CVE-2023-46280	Currently no fix is available
TIA Portal Cloud Connector: All versions < V2.0 affected by CVE-2023-46280	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109780755/
Totally Integrated Automation Portal (TIA Portal):	See below
Totally Integrated Automation Portal (TIA Portal) V18: All versions < V18 Update 4 affected by CVE-2023-46280	Update to V18 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109817218/
Totally Integrated Automation Portal (TIA Portal) V15.1: All versions affected by CVE-2023-46280	Currently no fix is planned
Totally Integrated Automation Portal (TIA Portal) V16: All versions affected by CVE-2023-46280	Currently no fix is planned
Totally Integrated Automation Portal (TIA Portal) V17: All versions affected by CVE-2023-46280	Currently no fix is available
Totally Integrated Automation Portal (TIA Portal) V19: All versions < V19 Update 2 affected by CVE-2023-46280	Update to V19 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109925643/

WORKAROUNDS AND MITIGATIONS

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

S7 PCT (Port Configuration Tool) is a PC-based software for parameterizing Siemens IO-Link master modules and third-party IO-Link devices.

Security Configuration Tool (SCT) is an engineering software for security devices such as SCALANCE-S or CP 443-1 Advanced.

SIMATIC Automation Tool allows commissioning, adjusting and service in combination with S7-1200 and S7-1500 Controllers without engineering framework.

SIMATIC NET PC software is a software product that is sold separately and implements the communications product from SIMATIC NET.

SIMATIC PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC, SIMATIC Batch, SIMATIC Route Control, OpenPCS 7 and other components.

SIMATIC PDM (Process Device Manager) is an universal, manufacturer-independent tool for configuration, parameter assignment, commissioning, diagnostics and maintenance of intelligent process devices (actors, sensors) and automation components (remote I/Os, multiplexer, process control units, compact controller).

SIMATIC STEP 7 V5 is the classic engineering software to configure and program SIMATIC S7-300/S7-400/C7/WinAC controllers.

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

SIMATIC WinCC Open Architecture (OA) is part of the SIMATIC HMI family. It is designed for use in applications requiring a high degree of customer-specific adaptability, large or complex applications and projects that impose specific system requirements or functions.

SIMATIC WinCC Runtime Advanced is a visualization runtime platform used for operator control and monitoring of machines and plants.

SIMATIC WinCC Runtime Professional is a visualization runtime platform used for operator control and monitoring of machines and plants.

SIMATIC WinCC Unified PC Runtime is the new visualization runtime platform used for operator control and monitoring of machines and plants.

SINAMICS Startdrive commissioning software is the engineering tool for integration of SINAMICS drives in TIA Portal.

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production environments.

SINUMERIK ONE is a digital-native CNC system with an integrated SIMATIC S7-1500 CPU for automation.

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.

TIA Portal Cloud Connector enables access to local PG/PC interfaces and connected SIMATIC hardware from the TIA Portal Engineering while the engineering is taking place via a remote desktop on a server of a private cloud.

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-2023-46280

The affected applications contain an out of bounds read vulnerability. This could allow an attacker to cause a Blue Screen of Death (BSOD) crash of the underlying Windows kernel.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	8.2
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H
CWE	CWE-125: Out-of-bounds Read

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Jongseong Kim, Byunghyun Kang, Sangjun Park, Yunjin Park, Kwon Yul, and Seungchan Kim from Team today-0day (bob 12th) 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 (2024-05-14):	Publication Date
V1.1 (2024-07-09):	Added fix for SIMATIC NET PC Software V18, SIMATIC WinCC Runtime Professional V16, V18, and V19 and SIMATIC WinCC V7.5, and V8.0, and TIA Portal V18

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.