

SSA-150063: Multiple Vulnerabilities in SINEC PNI before V2.0

Publication Date: 2023-11-14
Last Update: 2023-11-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

SINEC PNI before V2.0 is affected by multiple vulnerabilities.

Siemens has released an update for SINEC PNI and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEC PNI: All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109825079/

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

SINEC PNI (Primary Network Initialization) is program for initializing Siemens network components and Siemens controllers. In addition network-specific parameters, necessary for commissioning SCALANCE and RUGGEDCOM devices can be set.

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-2022-30184

.NET and Visual Studio Information Disclosure Vulnerability.

CVSS v3.1 Base Score 5.5
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2022-37434

zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to call inflateGetHeader (e.g., see the nodejs/node reference).

CVSS v3.1 Base Score 9.8
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-41032

NuGet Client Elevation of Privilege Vulnerability.

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:U/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2023-21808

.NET and Visual Studio Remote Code Execution Vulnerability

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](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2023-24895

.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability

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](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2023-24897

.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability

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](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2023-24936

.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability

CVSS v3.1 Base Score 7.5
CVSS Vector [CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2023-28260

.NET DLL Hijacking Remote Code Execution Vulnerability

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-20: Improper Input Validation

Vulnerability CVE-2023-29331

.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability

CVSS v3.1 Base Score 7.5
CVSS Vector [CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2023-32032

.NET and Visual Studio Elevation of Privilege Vulnerability

CVSS v3.1 Base Score 6.5
CVSS Vector [CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2023-33126

.NET and Visual Studio Remote Code Execution Vulnerability

CVSS v3.1 Base Score 7.3
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2023-33128

.NET and Visual Studio Remote Code Execution Vulnerability

CVSS v3.1 Base Score 7.3
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2023-33135

.NET and Visual Studio Elevation of Privilege Vulnerability

CVSS v3.1 Base Score 7.3
CVSS Vector [CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C](#)
CWE CWE-20: Improper Input Validation

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 (2023-11-14): 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.