SSA-892915: Multiple Denial of Service Vulnerabilities in the Webserver of Industrial Products

Publication Date: 2023-12-12
Last Update: 2023-12-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

Multiple vulnerabilities in the affected products could allow an unauthorized attacker with network access to the webserver to perform a denial of service attack.

Siemens has released a new version for SINAMICS S120 (incl. SIPLUS variants) 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 S7-400 CPU 412-2 PN V7 (6ES7412-2EK07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 414-3 PN/DP V7 (6ES7414-3EM07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 414F-3 PN/DP V7 (6ES7414-3FM07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416-3 PN/DP V7 (6ES7416-3ES07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 CPU 416F-3 PN/DP V7 (6ES7416-3FS07-0AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC PC-Station Plus: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SINAMICS S120 (incl. SIPLUS variants): All versions < V5.2 SP3 HF15	Update to V5.2 SP3 HF15 or later version https://support.industry.siemens.com/cs/ww/en/view/109780844/ See further recommendations from section Workarounds and Mitigations

SIPLUS S7-400 CPU 414-3 PN/DP V7 (6AG1414-3EM07-7AB0): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS S7-400 CPU 416-3 PN/DP V7 (6AG1416-3ES07-7AB0): All versions	Currently no fix is planned See 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:

- Disable the web server of the affected system
- Restrict access to webserver for trusted users only

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 PC Station is a software component that manages the SIMATIC software products and interfaces on a PC.

SIMATIC S7-400 controllers have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

With the SINAMICS converter series you can solve drive tasks in the low, medium and DC voltage range.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

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-2022-47374

The affected products do not handle HTTP(S) requests to the web server correctly.

This could allow an attacker to exhaust system resources and create a denial of service condition for the device.

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-674: Uncontrolled Recursion

Vulnerability CVE-2022-47375

The affected products do not handle long file names correctly.

This could allow an attacker to create a buffer overflow and create a denial of service condition for the device.

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-805: Buffer Access with Incorrect Length Value

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 (2023-12-12):	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.