

**SSA-557541: Denial-of-Service Vulnerability in SIMATIC S7-400 CPUs**

Publication Date: 2022-04-12  
 Last Update: 2023-04-11  
 Current Version: V1.2  
 CVSS v3.1 Base Score: 7.5

**SUMMARY**

SIMATIC S7-400 CPU devices contain an input validation vulnerability that could allow an attacker to create a Denial-of-Service condition. A restart is needed to restore normal operations.

Siemens has released an update for SIMATIC S7-410 V10 CPU family and SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants for both) and recommends to update to the latest version. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not yet available.

**AFFECTED PRODUCTS AND SOLUTION**

Affected Product and Versions	Remediation
SIMATIC S7-400 CPU 412-1 DP V7 (6ES7412-1XJ07-0AB0): All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 CPU 412-2 DP V7 (6ES7412-2XK07-0AB0): All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 CPU 412-2 PN/DP V7 (6ES7412-2EK07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109752685/">https://support.industry.siemens.com/cs/ww/en/view/109752685/</a> See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 CPU 414-2 DP V7 (6ES7414-2XL07-0AB0): All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 CPU 414-3 DP V7 (6ES7414-3XM07-0AB0): All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 CPU 414-3 PN/DP V7 (6ES7414-3EM07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109752685/">https://support.industry.siemens.com/cs/ww/en/view/109752685/</a> See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 CPU 414F-3 PN/DP V7 (6ES7414-3FM07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109752685/">https://support.industry.siemens.com/cs/ww/en/view/109752685/</a> See recommendations from section <a href="#">Workarounds and Mitigations</a>

SIMATIC S7-400 CPU 416-2 DP V7 (6ES7416-2XP07-0AB0): All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 CPU 416-3 DP V7 (6ES7416-3XS07-0AB0): All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 CPU 416-3 PN/DP V7 (6ES7416-3ES07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109752685/">https://support.industry.siemens.com/cs/ww/en/view/109752685/</a> See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 CPU 416F-2 DP V7 (6ES7416-2FP07-0AB0): All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 CPU 416F-3 PN/DP V7 (6ES7416-3FS07-0AB0): All versions < V7.0.3	Update to V7.0.3 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109752685/">https://support.industry.siemens.com/cs/ww/en/view/109752685/</a> See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 CPU 417-4 DP V7 (6ES7417-4XT07-0AB0): All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants): All versions < V6.0.10	Update to V6.0.10 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109474550/">https://support.industry.siemens.com/cs/ww/en/view/109474550/</a> See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants): All versions < V8.2.3	Update to V8.2.3 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109476571/">https://support.industry.siemens.com/cs/ww/en/view/109476571/</a> See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants): All versions < V10.1	Update to V10.1 or later version To obtain SIMATIC S7-410 V10.1 contact your local support. See further recommendations from section <a href="#">Workarounds and Mitigations</a>
SIPLUS S7-400 CPU 414-3 PN/DP V7 (6AG1414-3EM07-7AB0): All versions < V7.0.3	Update to V7.0.3 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109752685/">https://support.industry.siemens.com/cs/ww/en/view/109752685/</a> See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIPLUS S7-400 CPU 416-3 PN/DP V7 (6AG1416-3ES07-7AB0): All versions < V7.0.3	Update to V7.0.3 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109752685/">https://support.industry.siemens.com/cs/ww/en/view/109752685/</a> See recommendations from section <a href="#">Workarounds and Mitigations</a>

SIPLUS S7-400 CPU 416-3 V7 (6AG1416-3XS07-7AB0): All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>
SIPLUS S7-400 CPU 417-4 V7 (6AG1417-4XT07-7AB0): All versions	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>

## **WORKAROUNDS AND MITIGATIONS**

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

- Limit access to port 102/tcp to trusted users and systems 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 S7-400 controllers have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

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-2021-40368**

Affected devices improperly handle specially crafted packets sent to port 102/tcp.

This could allow an attacker to create a Denial-of-Service condition. A restart is needed to restore normal operations.

CVSS v3.1 Base Score	7.5
CVSS Vector	<a href="#">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</a>
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

### **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 (2022-04-12):	Publication Date
V1.1 (2022-08-09):	Added fix for SIMATIC S7-410 CPU family
V1.2 (2023-04-11):	Added explicit MLFBs and fixes for SIMATIC S7-400 V7 CPUs (incl. SIPLUS variants)

### **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](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.