SSA-566905: Multiple Denial of Service Vulnerabilities in the Webserver of Industrial Products

Publication Date: 2023-04-11
Last Update: 2024-06-11
Current Version: V1.2
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 of an affected products to perform a denial of service attack.

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 specific countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 443-1 (6GK7443-1EX30-0XE0): All versions < V3.3 affected by all CVEs	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 (6GK7443-1EX30-0XE1): All versions < V3.3 affected by all CVEs	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 Advanced (6GK7443-1GX30-0XE0): All versions < V3.3 affected by all CVEs	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1242-7 V2 (6GK7242-7KX31-0XE0): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 (6GK7243-1BX30-0XE0): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-1 DNP3 (incl. SIPLUS variants): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations

SIMATIC CP 1243-1 IEC (incl. SIPLUS variants): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-7 LTE EU (6GK7243-7KX30-0XE0): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-7 LTE US (6GK7243-7SX30-0XE0): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1243-8 IRC (6GK7243-8RX30-0XE0): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 1542SP-1 (6GK7542-6UX00-0XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1542SP-1 IRC (6GK7542-6VX00-0XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/ See further recommendations from section Workarounds and Mitigations
SIMATIC CP 1543SP-1 (6GK7543-6WX00-0XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CP 1542SP-1 IRC TX RAIL (6AG2542-6VX00-4XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CP 1543SP-1 ISEC (6AG1543-6WX00-7XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/ See further recommendations from section Workarounds and Mitigations
SIPLUS ET 200SP CP 1543SP-1 ISEC TX RAIL (6AG2543-6WX00-4XE0): All versions < V2.3 affected by all CVEs	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109954475/ See further recommendations from section Workarounds and Mitigations

SIPLUS NET CP 443-1 (6AG1443-1EX30-4XE0): All versions < V3.3 affected by all CVEs	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET CP 443-1 Advanced (6AG1443-1GX30-4XE0): All versions < V3.3 affected by all CVEs	Update to V3.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109817938/ See further recommendations from section Workarounds and Mitigations
SIPLUS NET CP 1242-7 V2 (6AG1242-7KX31-7XE0): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS S7-1200 CP 1243-1 (6AG1243-1BX30-2AX0): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS S7-1200 CP 1243-1 RAIL (6AG2243-1BX30-1XE0): All versions affected by all CVEs	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIPLUS TIM 1531 IRC (6AG1543-1MX00-7XE0): All versions < V2.3.6 affected by all CVEs	Update to V2.3.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109817397/ See further recommendations from section Workarounds and Mitigations
TIM 1531 IRC (6GK7543-1MX00-0XE0): All versions < V2.3.6 affected by all CVEs	Update to V2.3.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109817397/ 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:

- Deactivate the webserver if not required, and if deactivation is supported by the product
- Restrict access to the web interface of the affected products, if deactivation is not supported by the product

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 CP 1242-7 and CP 1243-7 LTE communications processors connect SIMATIC S7-1200 controllers to Wide Area Networks (WAN). They provide integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

SIMATIC CP 1243-8 IRC communications processors connect SIMATIC S7-1200 controllers via the SINAUT ST7 telecontrol protocol to a control center or master ST7 stations.

SIMATIC CP 1243-1 communications processors connect S7-1200 controllers to Ethernet networks. They provide integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

SIMATIC CP 1543-1, CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communications processors connect SIMATIC S7-1500 controllers to Ethernet networks. They provide integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

SIMATIC CP 343-1 and CP 443-1 are communication processors (CP) designed to enable Ethernet communication for SIMATIC S7-300/S7-400 CPUs.

SIMATIC IPC DiagBase diagnostics software allows to recognize early on any potential faults on SIMATIC IPCs and helps to avoid or reduce system downtimes.

SIMATIC IPC DiagMonitor monitors, reports, visualizes and logs the system states of the SIMATIC IPCs. It communicates with other systems and reacts when events occur.

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7, DNP3 and IEC 60870-5-101/104 with three RJ45 interfaces for communication via IP-based networks (WAN / LAN) and a RS 232/RS 485 interface for communication via classic WAN networks.

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-2022-43716

The webserver of the affected products contains a vulnerability that may lead to a denial of service condition. An attacker may cause a denial of service situation which leads to a restart of the webserver of the affected product.

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-416: Use After Free

Vulnerability CVE-2022-43767

The webserver of the affected products contains a vulnerability that may lead to a denial of service condition. An attacker may cause a denial of service situation of the webserver of the affected product.

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-833: Deadlock

Vulnerability CVE-2022-43768

The webserver of the affected products contains a vulnerability that may lead to a denial of service condition. An attacker may cause a denial of service situation of the webserver of the affected product.

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-770: Allocation of Resources Without Limits or Throttling

ADDITIONAL INFORMATION

These vulnerabilities have been discovered internally by Siemens.

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 (2023-04-11):	Publication Date
V1.1 (2023-05-09):	Removed SIMATIC IPC DiagBase and SIMATIC IPC DiagMonitor as they are not affected
V1.2 (2024-06-11):	Added fixes for SIMATIC CP 15xxSP-1 devices

TERMS OF USE