SSA-384224: Denial of Service Vulnerability in SIMATIC HMI Panels

Publication Date:	2022-10-11
Last Update:	2022-10-11
Current Version:	V1.0
CVSS v3.1 Base Score:	7.5

SUMMARY

Several SIMATIC HMI Panels are affected by a vulnerability that could allow an attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC HMI Comfort Panels (incl. SIPLUS variants): All versions < V17 Update 4	Update to V17 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/ See further recommendations from section Workarounds and Mitigations
SIMATIC HMI KTP400 Basic (6AV2123-2DB03-0AX0): All versions < V17 Update 5	Update to V17 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/ See further recommendations from section Workarounds and Mitigations
SIMATIC HMI KTP700 Basic (6AV2123-2GB03-0AX0): All versions < V17 Update 5	Update to V17 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/ See further recommendations from section Workarounds and Mitigations
SIMATIC HMI KTP900 Basic (6AV2123-2JB03-0AX0): All versions < V17 Update 5	Update to V17 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/ See further recommendations from section Workarounds and Mitigations
SIMATIC HMI KTP1200 Basic (6AV2123-2MB03-0AX0): All versions < V17 Update 5	Update to V17 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/ See further recommendations from section Workarounds and Mitigations
SIMATIC HMI KTP Mobile Panels: All versions < V17 Update 4	Update to V17 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/ See further recommendations from section Workarounds and Mitigations
SIPLUS HMI KTP400 BASIC (6AG1123-2DB03-2AX0): All versions < V17 Update 5	Update to V17 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/ See further recommendations from section Workarounds and Mitigations

SIPLUS HMI KTP700 BASIC (6AG1123-2GB03-2AX0): All versions < V17 Update 5	Update to V17 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/ See further recommendations from section Workarounds and Mitigations
SIPLUS HMI KTP900 BASIC (6AG1123-2JB03-2AX0): All versions < V17 Update 5	Update to V17 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/ See further recommendations from section Workarounds and Mitigations
SIPLUS HMI KTP1200 BASIC (6AG1123-2MB03-2AX0): All versions < V17 Update 5	Update to V17 Update 5 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/ 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:

- Restrict access to port 5001/tcp and 5002/tcp to trusted IP addresses 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 HMI Panels are used for operator control and monitoring of machines and plants.

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-2022-40227

Affected devices do not properly validate input sent to certain services over TCP. This could allow an unauthenticated remote attacker to cause a permanent denial of service condition (requiring a device reboot) by sending specially crafted TCP packets.

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

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Cyber Research Group from Raytheon UK 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 (2022-10-11):	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.