# SSA-364335: Clear Text Transmission Vulnerability on SIMATIC HMI Panels

Publication Date: 2020-07-14
Last Update: 2020-07-14
Current Version: V1.0
CVSS v3.1 Base Score: 5.7

## SUMMARY

A clear text transmission vulnerability in SIMATIC HMI panels could allow an attacker to access sensitive information under certain circumstances.

Siemens recommends specific countermeasures to mitigate this vulnerability.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SIMATIC HMI Basic Panels 1st Generation (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI Comfort Panels (incl. SIPLUS variants):<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI KTP700F Mobile Arctic:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC HMI Mobile Panels 2nd Generation:<br>All versions | See recommendations from section Workarounds and Mitigations |
| SIMATIC WinCC Runtime Advanced:<br>All versions | 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:

- Avoid program transfer over large networks to prevent an attacker from sniffing potential unencrypted traffic.
- As much as possible, connect the Engineering Station (or device with the WinCC Engineering software) directly to the HMI without using any network device in between.

## 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.

SIMATIC WinCC Runtime Advanced is a visualization runtime platform 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-2020-7592

Unencrypted communication between the configuration software and the respective device could allow an attacker to capture potential plain text communication and have access to sensitive information.

| | |
|---|---|
| CVSS v3.1 Base Score | 5.7 |
| CVSS Vector | CVSS:3.1/AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N/E:P/RL:W/RC:C |
| CWE | CWE-319: Cleartext Transmission of Sensitive Information |

## ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Richard Thomas and Tom Chothia from University of Birmingham for coordinated disclosure

## 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 (2020-07-14): 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.