SSA-520004: Telnet Authentication Vulnerability in SIMATIC HMI Comfort Panels

Publication Date: 2021-01-28
Last Update: 2021-01-28
Current Version: V1.0
CVSS v3.1 Base Score: 8.1

SUMMARY

SIMATIC HMI Panels are affected by a vulnerability that could allow a remote attacker to gain full access to the device(s), if the telnet service is enabled.

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 < V16 Update 3a	Update to V16 Update 3a or later version https://support.industry.siemens.com/cs/ww/en/view/109746530
SIMATIC HMI KTP Mobile Panels: All versions < V16 Update 3a	Update to V16 Update 3a or later version https://support.industry.siemens.com/cs/ww/en/view/109746530

WORKAROUNDS AND MITIGATIONS

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

- Disable telnet on the HMI Panels if enabled. Note: By default telnet is disabled.

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-2020-15798

Affected devices with enabled telnet service do not require authentication for this service. This could allow a remote attacker to gain full access to the device. (ZDI-CAN-12046)

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure

- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts

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 (2021-01-28):   Publication Date

TERMS OF USE