SSA-542525: Authentication Vulnerabilities in SIMATIC HMI Products

Publication Date: 2020-09-08
Last Update: 2020-09-08
Current Version: V1.0
CVSS v3.1 Base Score: 6.5

SUMMARY

SIMATIC HMI Products are affected by two vulnerabilities that could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack.

Siemens is preparing updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC HMI Basic Panels 2nd Generation (incl. SIPLUS variants): All versions >= 14 and V < XX only affected by CVE-2020-15786	See recommendations from section Workarounds and Mitigations
SIMATIC HMI Comfort Panels (incl. SIPLUS variants): All versions only affected by CVE-2020-15786	See recommendations from section Workarounds and Mitigations
SIMATIC HMI Mobile Panels: All versions only affected by CVE-2020-15786	See recommendations from section Workarounds and Mitigations
SIMATIC HMI United Comfort Panels: 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:

- Apply Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security

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-2020-15786

Affected devices insufficiently block excessive authentication attempts.

This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L/E:P/RL:W/RC:C
CWE	CWE-307: Improper Restriction of Excessive Authentication Attempts

Vulnerability CVE-2020-15787

Affected devices insufficiently validate authentication attempts as the information given can be truncated to match only a set number of characters versus the whole provided string.

This could allow a remote attacker to discover user passwords and obtain access to the Sm@rt Server via a brute-force attack.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:U/RC:C
CWE	CWE-305: Authentication Bypass by Primary Weakness

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Joseph Gardiner from Bristol Cyber Security Group - University of Bristol for reporting the vulnerabilties

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 (2020-09-08): Publication Date

TERMS OF USE