SSA-542701: Vulnerabilities in SIEMENS LOGO!

Publication Date: 2019-05-14
Last Update: 2020-12-08
Current Version: V1.2
CVSS v3.1 Base Score: 9.4

SUMMARY

Multiple vulnerabilities have been identified in SIEMENS LOGO!8 BM devices. The most severe vulnerability could lead to an attacker reading and modifying the device configuration if the attacker has access to port 10005/tcp.

Siemens has released an update for the LOGO! 8 BM (incl. SIPLUS variants) and recommends that customers update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
LOGO! 8 BM (incl. SIPLUS variants): All versions < V8.3	Update to V8.3. Notice that in order to update, a new hardware version is required. https://support.industry.siemens.com/cs/ww/en/view/109783346/

WORKAROUNDS AND MITIGATIONS

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

- Apply Defense-in-Depth concept, including protection concept outlined in the system manual.

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

Siemens LOGO! BM (Base Module) devices are used for basic small-scale automation tasks.

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-2019-10919

Attackers with access to port 10005/tcp could perform device reconfigurations and obtain project files from the devices. The system manual recommends to protect access to this port.

The security vulnerability could be exploited by an unauthenticated attacker with network access to port 10005/tcp. No user interaction is required to exploit this security vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	9.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:F/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2019-10920

Project data stored on the device, which is accessible via port 10005/tcp, can be decrypted due to a hardcoded encryption key.

The security vulnerability could be exploited by an unauthenticated attacker with network access to port 10005/tcp. No user interaction is required to exploit this security vulnerability. The vulnerability impacts confidentiality of the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C
CWE	CWE-321: Use of Hard-coded Cryptographic Key

Vulnerability CVE-2019-10921

Unencrypted storage of passwords in the project could allow an attacker with access to port 10005/tcp to obtain passwords of the device.

The security vulnerability could be exploited by an unauthenticated attacker with network access to port 10005/tcp. No user interaction is required to exploit this security vulnerability. The vulnerability impacts confidentiality of the device.

At the time of advisory publication no public exploitation of this security vulnerability was known

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:O/RC:C
CWE	CWE-256: Unprotected Storage of Credentials

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Manuel Stotz and Matthias Deeg from SySS GmbH for coordinated disclosure
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2019-05-14): Publication Date
V1.1 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products
V1.2 (2020-12-08): Add solution for LOGO! 8 BM

TERMS OF USE