

SSA-542701: Vulnerabilities in SIEMENS LOGO!

Publication Date: 2019-05-14
Last Update: 2019-05-14
Current Version: V1.0
CVSS v3.0 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.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
LOGO!8 BM: 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 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](#)), 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! devices are used for basic small-scale automation tasks.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (<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.

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 v3.0 Base Score 9.4
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:F/RL:U/RC:C

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 v3.0 Base Score 7.5
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:U/RC:C

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 v3.0 Base Score 7.5
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:F/RL:U/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Manuel Stotz and Matthias Deeg from SySS GmbH 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 (2019-05-14): 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.