SSA-087240: Vulnerabilities in SIEMENS LOGO!

Publication Date	2017-08-30
Last Update	2017-08-30
Current Version	V1.0
CVSS v3.0 Base Score	7.5

SUMMARY

Two vulnerabilities have been identified in SIEMENS LOGO!8 BM devices. The most severe vulnerability could allow an attacker to hijack existing web sessions.

Siemens provides LOGO!8 BM FS-05 with firmware version V1.81.2, which fixes the first vulnerability, and recommends specific mitigations for the second vulnerability.

AFFECTED PRODUCTS

- LOGO!8 BM: All versions < V1.81.2 (Vulnerability CVE-2017-12734)
- LOGO!8 BM: All versions (Vulnerability CVE-2017-12735)

DESCRIPTION

Siemens LOGO! devices are used for basic small-scale automation tasks.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2017-12734)

An attacker with network access to the integrated web server on port 80/tcp could obtain the session ID of an active user session. A user must be logged in to the web interface. Siemens recommends to use the integrated webserver on port 80/tcp only in trusted networks.

CVSS 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:P/RL:O/RC:C

Vulnerability 2 (CVE-2017-12735)

An attacker who performs a Man-in-the-Middle attack between the LOGO! BM and other devices could potentially decrypt and modify network traffic.

CVSS Base Score	7.4
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:T/RC:C

SOLUTION

Siemens provides LOGO!8 BM FS-05 with firmware version V1.81.2, which fixes the first vulnerability.

Siemens recommends applying the following mitigations for customers with existing installations, and for mitigation of the second vulnerability:

- Configure the environment according to the recommendations in the user manual [1]
- Apply cell protection concept [2]

- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth [3]

As a general security measure Siemens strongly recommends to protect network access to the devices with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [2] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks Maxim Rupp for coordinated disclosure of vulnerability 1.

ADDITIONAL RESOURCES

[1] LOGO!8 BM User manual can be obtained from:
https://support.industry.siemens.com/cs/us/en/view/109741041

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[3] Further information about Defense-in-Depth:
http://www.industry.siemens.com/topics/global/en/industrial-security/concept/Pages/defense-in-depth.aspx

[4] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[5] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2017-08-30):	Publication Date

DISCLAIMER

See: https://www.siemens.com/terms_of_use