SSA-087240: Vulnerabilities in SIEMENS LOGO!

Publication Date: 2017-08-30
Last Update: 2020-12-08
Current Version: V1.2
CVSS v3.1 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 has released updates for the affected products 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 < V1.81.2 only affected by CVE-2017-12734	Siemens provides LOGO!8 BM FS-05 with firmware version V1.81.2, which fixes CVE-2017-12734
LOGO! 8 BM (incl. SIPLUS variants): All versions < V8.3 only affected by CVE-2017-12735	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:

- Configure the environment according to the recommendations in the user manual (see https://support.industry.siemens.com/cs/us/en/view/109741041)
- Apply cell protection concept (see https://www.siemens.com/cert/operational-guidelines-industrial-security)
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth (see http://www.industry.siemens.com/topics/global/en/industrial-security/concept/Pages/defense-in-depth.aspx)

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-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 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:P/RL:O/RC:C
CWE	CWE-895: SFP Primary Cluster: Information Leak

Vulnerability 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 v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-300: Channel Accessible by Non-Endpoint

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Maxim Rupp for coordinated disclosure of CVE-2017-12734
- 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 (2017-08-30): 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 CVE-2017-12735.

TERMS OF USE