SSA-928782: Firmware Authenticity Vulnerability in LOGO! 8 BM Devices

Publication Date: 2022-10-11
Last Update: 2022-10-11
Current Version: V1.0
CVSS v3.1 Base Score: 6.1

SUMMARY

LOGO! 8 BM (incl. SIPLUS variants) contains a vulnerability that could allow an attacker to install manipulated firmware packages.

Siemens has released an update for the LOGO! 8 BM (incl. SIPLUS variants) and recommends to 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 or later version. Note that in order to update, a new hardware version is required https://support.industry.siemens.com/cs/ww/en/view/109783346/ See further 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:

- Be especially careful to obtain and install firmware upgrades only from official sources

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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-2022-36360

Affected devices load firmware updates without checking the authenticity. Furthermore the integrity of the unencrypted firmware is only verified by a non-cryptographic method. This could allow an attacker to manipulate a firmware update and flash it to the device.

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-345: Insufficient Verification of Data Authenticity

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Cyber Research Group from Raytheon UK for reporting the vulnerabilities

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 (2022-10-11): 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.