SSA-573753: Remote Code Execution in Siemens LOGO! Web Server

Publication Date: 2020-07-14
Last Update: 2020-07-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

The latest update for LOGO! 8 BM devices fixes a vulnerability that could allow remote code execution in the web server functionality.

Siemens provides a firmware update for the latest versions of LOGO! BM.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
LOGO! 8 BM (incl. SIPLUS variants): V1.81.01 - V1.81.03	Update to V1.81.04 https://support.industry.siemens.com/cs/ww/en/view/109780764/
LOGO! 8 BM (incl. SIPLUS variants): V1.82.01	Update to V1.82.03 https://support.industry.siemens.com/cs/ww/en/view/109780764/
LOGO! 8 BM (incl. SIPLUS variants): V1.82.02	Update to V1.82.04 https://support.industry.siemens.com/cs/ww/en/view/109780764/

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-2020-7593

A buffer overflow vulnerability exists in the Web Server functionality of the device. A remote unauthenticated attacker could send a specially crafted HTTP request to cause a memory corruption, potentially resulting in remote code execution.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Alexander Perez-Palma and Dave McDaniel from Cisco Talos for coordinated disclosure
- Emanuel Almeida from Cisco Systems, Inc 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 (2020-07-14): Publication Date

TERMS OF USE