SSA-783481: Denial-of-Service Vulnerability in LOGO! 8 BM

Publication Date: 2021-03-09
Last Update: 2024-10-08
Current Version: V1.3
CVSS v3.1 Base Score: 5.5

SUMMARY

A Denial-of-Service vulnerability has been identified in LOGO! 8 BM. This vulnerability could allow an attacker to crash a device, if a user is tricked into loading a malicious project file onto an affected device.

The vulnerability is related to the hardware of the product. Siemens has released new hardware versions with the LOGO! V8.4 BM and the SIPLUS LOGO! V8.4 BM product families for all affected devices in which this vulnerability is fixed. See the chapter “Additional Information” below for more details.

For more information please also refer to the related product support article: https://support.industry.siemens.com/cs/ww/en/view/109826554/.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
LOGO! V8.3 BM:	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 12/24RCE (6ED1052-1MD08-0BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 12/24RCEo (6ED1052-2MD08-0BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 230RCE (6ED1052-1FB08-0BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 230RCEo (6ED1052-2FB08-0BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24CE (6ED1052-1CC08-0BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24CEo (6ED1052-2CC08-0BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations

LOGO! 24RCE (6ED1052-1HB08-0BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24RCEo (6ED1052-2HB08-0BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! V8.3 BM:	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 12/24RCEo (6AG1052-2MD08-7BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 230RCE (6AG1052-1FB08-7BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 230RCEo (6AG1052-2FB08-7BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24CE (6AG1052-1CC08-7BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA1): All versions affected by CVE-2020-25236	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24RCEo (6AG1052-2HB08-7BA1): All versions affected by CVE-2020-25236	Currently no fix is planned 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:

- Siemens recommends limiting the possibilities to execute untrusted code if possible.

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 DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2020-25236

The control logic (CL) the LOGO! 8 executes could be manipulated in a way that could cause the device executing the CL to improperly handle the manipulation and crash. After successful execution of the attack, the device needs to be manually reset.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:T/RC:C
CWE	CWE-755: Improper Handling of Exceptional Conditions

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Max Bäumler for coordinated disclosure

ADDITIONAL INFORMATION

Siemens has released new hardware versions with the LOGO! V8.4 BM and the SIPLUS LOGO! V8.4 BM product families for all affected devices in which the vulnerability is fixed:

- LOGO! 12/24RCE (6ED1052-1MD08-0BA2)
- LOGO! 12/24RCEo (6ED1052-2MD08-0BA2)
- LOGO! 230RCE (6ED1052-1FB08-0BA2)
- LOGO! 230RCEo (6ED1052-2FB08-0BA2)
- LOGO! 24CE (6ED1052-1CC08-0BA2)
- LOGO! 24CEo (6ED1052-2CC08-0BA2)
- LOGO! 24RCE (6ED1052-1HB08-0BA2)
- LOGO! 24RCEo (6ED1052-2HB08-0BA2)
- SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA2)
- SIPLUS LOGO! 12/24RCEo (6AG1052-2MD08-7BA2)
- SIPLUS LOGO! 230RCE (6AG1052-1FB08-7BA2)
- SIPLUS LOGO! 230RCEo (6AG1052-2FB08-7BA2)
- SIPLUS LOGO! 24CE (6AG1052-1CC08-7BA2)
- SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA2)
- SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA2)
- SIPLUS LOGO! 24RCEo (6AG1052-2HB08-7BA2)

For more information please also refer to the related product support article: https://support.industry.siemens.com/cs/ww/en/view/109826554/.

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 (2021-03-09):	Publication Date
V1.1 (2023-12-12):	Added information about additional new LOGO! V8.4 BM hardware versions
V1.2 (2024-09-10):	Added information about additional new SIPLUS LOGO! hardware versions: SIPLUS LOGO! 24CE and SIPLUS LOGO! 230RCE
V1.3 (2024-10-08):	Added information about additional new SIPLUS LOGO! hardware versions

TERMS OF USE