SSA-955858: Multiple Vulnerabilities in LOGO! 8 BM Devices

Publication Date:	2022-10-11
Last Update:	2023-12-12
Current Version:	V1.1
CVSS v3.1 Base Score:	9.8

SUMMARY

LOGO! 8 BM (incl. SIPLUS variants) contains multiple web-related vulnerabilities. These could allow an attacker to execute code remotely, put the device into a denial of service state or retrieve parts of the memory.

The vulnerabilities are related to the hardware of the product. Siemens has released new hardware versions with the LOGO! V8.4 BM product family for several affected devices in which several of those vulnerabilities are fixed. Siemens is working on new hardware versions for the SIPLUS devices to address this issue further. 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! 12/24RCE (6ED1052-1MD08-0BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 12/24RCE (6ED1052-1MD08-0BA2): All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 12/24RCEo (6ED1052-2MD08-0BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 12/24RCEo (6ED1052-2MD08-0BA2): All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24CE (6ED1052-1CC08-0BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24CE (6ED1052-1CC08-0BA2): All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24CEo (6ED1052-2CC08-0BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

LOGO! 24CEo (6ED1052-2CC08-0BA2): All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24RCE (6ED1052-1HB08-0BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24RCE (6ED1052-1HB08-0BA2): All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24RCEo (6ED1052-2HB08-0BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24RCEo (6ED1052-2HB08-0BA2): All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 230RCE (6ED1052-1FB08-0BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 230RCE (6ED1052-1FB08-0BA2): All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 230RCEo (6ED1052-2FB08-0BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 230RCEo (6ED1052-2FB08-0BA2): All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 12/24RCE: All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 12/24RCE (6AG1052-1MD08-7BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 12/24RCEo: All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIPLUS LOGO! 12/24RCEo (6AG1052-2MD08-7BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24CE: All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24CE (6AG1052-1CC08-7BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24CEo: All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24CEo (6AG1052-2CC08-7BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24RCE: All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24RCE (6AG1052-1HB08-7BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24RCEo: All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 24RCEo (6AG1052-2HB08-7BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 230RCE: All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 230RCE (6AG1052-1FB08-7BA1): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS LOGO! 230RCEo: All versions affected by CVE-2022-36362	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIPLUS LOGO! 230RCEo (6AG1052-2FB08-7BA1): All versions	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:

- Only for versions < V8.3: Restrict access to port 10005/tcp to trusted IP addresses only
- Only for versions >= V8.3: Restrict access to port 8443/tcp to trusted IP addresses only
- Restrict access to port 135/tcp to trusted IP addresses only

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-2022-36361

Affected devices do not properly validate the structure of TCP packets in several methods. This could allow an attacker to cause buffer overflows, get control over the instruction counter and run custom code.

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:T/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-36362

Affected devices do not conduct certain validations when interacting with them. This could allow an unauthenticated remote attacker to manipulate the devices IP address, which means the device would not be reachable and could only be recovered by power cycling the device.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:T/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2022-36363

Affected devices do not properly validate an offset value which can be defined in TCP packets when calling a method. This could allow an attacker to retrieve parts of the content of the memory.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:T/RC:C
CWE	CWE-1285: Improper Validation of Specified Index, Position, or Offset in Input

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Cyber Research Group from Raytheon UK for reporting the vulnerabilities

ADDITIONAL INFORMATION

Siemens has released new hardware versions with the LOGO! V8.4 BM product family for several affected devices. Those new hardware versions fixes the vulnerabilities CVE-2022-36361 and CVE-2022-36363:

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

Siemens is working on new hardware versions for the SIPLUS devices to address this issue further.

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 (2022-10-11):	Publication Date
V1.1 (2023-12-12):	Added information about additional new LOGO! V8.4 BM hardware versions

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.