

SSA-844582: Electromagnetic Fault Injection in LOGO! V8.3 BM Devices Results in Broken LOGO! V8.3 Product CA

Publication Date: 2023-12-12
Last Update: 2023-12-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.6

SUMMARY

LOGO! V8.3 BM (incl. SIPLUS variants) devices contain a vulnerability that could allow an electromagnetic fault injection. This could allow an attacker to dump and debug the firmware, including the manipulation of memory. Further actions could allow to inject public keys of custom created key pairs which are then signed by the LOGO! V8.3 Product CA.

The vulnerability is related to the specific hardware architecture of the LOGO! V8.3 BM. Siemens has released new hardware versions with the LOGO! V8.4 BM product family for several affected devices in which the vulnerability is fixed and the Product CA private key is rotated. 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 >= V8.3	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 12/24RCEo (6ED1052-2MD08-0BA1): All versions >= V8.3	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24CE (6ED1052-1CC08-0BA1): All versions >= V8.3	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24CEo (6ED1052-2CC08-0BA1): All versions >= V8.3	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24RCE (6ED1052-1HB08-0BA1): All versions >= V8.3	Currently no fix is planned See recommendations from section Workarounds and Mitigations
LOGO! 24RCEo (6ED1052-2HB08-0BA1): All versions >= V8.3	Currently no fix is planned See recommendations from section Workarounds and Mitigations

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

- Use HTTPS communication only in trusted networks without unknown network devices
- If possible, connect the Base Module directly with LOGO! Soft Comfort and the Web Browser

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-2022-42784

Affected devices are vulnerable to an electromagnetic fault injection. This could allow an attacker to dump and debug the firmware, including the manipulation of memory. Further actions could allow to inject public keys of custom created key pairs which are then signed by the product CA. The generation of a custom certificate allows communication with, and impersonation of, any device of the same version.

CVSS v3.1 Base Score	7.6
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-1319: Improper Protection against Electromagnetic Fault Injection (EM-FI)

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Sebastien Leger for reporting the vulnerability

ADDITIONAL INFORMATION

Siemens has released new hardware versions with the LOGO! V8.4 BM product family for several affected devices in which the vulnerability is fixed and the Product CA private key is rotated:

- 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 (2023-12-12): 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.