SSA-102144: Code Execution Vulnerability in LOGO! Soft Comfort

Publication Date: 2019-05-14
Last Update: 2020-12-08
Current Version: V1.1
CVSS v3.1 Base Score: 7.8

SUMMARY

A vulnerability was identified in LOGO! Soft Comfort. The vulnerability could allow an attacker to execute arbitrary code if the attacker tricks a legitimate user to open a manipulated project.

Siemens has released an update for the LOGO! Soft Comfort and recommends that customers update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
LOGO! Soft Comfort: All versions < V8.3	Updated to V8.3 https://support.industry.siemens.com/cs/ww/en/view/109783154/

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Only open projects from trusted sources.

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

LOGO! Soft Comfort is an engineering software to configure and program LOGO! BM (Base Module) devices

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-2019-10924

The vulnerability could allow an attacker to execute arbitrary code if the attacker tricks a legitimate user to open a manipulated project.

In order to exploit the vulnerability, a valid user must open a manipulated project file. No further privileges are required on the target system. The vulnerability could compromise the confidentiality, integrity and availability of the engineering station.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-502: Deserialization of Untrusted Data

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- axt for reporting the vulnerability.
- iDefense Labs for reporting the vulnerability and coordination efforts.

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 (2019-05-14): Publication Date
V1.1 (2020-12-08): Added solution

TERMS OF USE