

## **SSA-983300: Vulnerabilities in LOGO! Soft Comfort**

Publication Date: 2021-04-13  
Last Update: 2023-12-12  
Current Version: V1.1  
CVSS v3.1 Base Score: 8.4

### **SUMMARY**

Two vulnerabilities have been identified in the LOGO! Soft Comfort software. These could allow an attacker to take over a system with the affected software installed.

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

### **AFFECTED PRODUCTS AND SOLUTION**

Affected Product and Versions	Remediation
LOGO! Soft Comfort: All versions < V8.4	Update to V8.4 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109826553/">https://support.industry.siemens.com/cs/ww/en/view/109826553/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

### **WORKAROUNDS AND MITIGATIONS**

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

- If possible do not execute the LOGO! Soft Comfort software with administrative privileges
- Restrict access to project files on the engineering station to trusted users
- Import only project files from trusted sources

Product-specific remediations or mitigations can be found in the section [Affected Products and Solution](#). 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**

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-2020-25243**

A zip slip vulnerability could be triggered while importing a compromised project file to the affected software. Chained with other vulnerabilities this vulnerability could ultimately lead to a system takeover by an attacker.

CVSS v3.1 Base Score	5.1
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L/E:P/RL:U/RC:C</a>
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

### **Vulnerability CVE-2020-25244**

The software insecurely loads libraries which makes it vulnerable to DLL hijacking. Successful exploitation by a local attacker could lead to a takeover of the system where the software is installed.

CVSS v3.1 Base Score	8.4
CVSS Vector	<a href="#">CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C</a>
CWE	CWE-427: Uncontrolled Search Path Element

## **ACKNOWLEDGMENTS**

Siemens thanks the following party for its efforts:

- Mashav Sapir from Claroty 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 (2021-04-13): Publication Date  
V1.1 (2023-12-12): Added fix for LOGO! Soft Comfort

## **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](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.