SSA-983300: Vulnerabilities in LOGO! Soft Comfort

Publication Date: 2021-04-13
Last Update: 2021-04-13
Current Version: V1.0
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 is preparing updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
LOGO! Soft Comfort: All versions	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:

- 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

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	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
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	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
CWE	CWE-427: Uncontrolled Search Path Element

ACKNOWLEDGMENTS

Siemens thanks the following parties for their 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

TERMS OF USE