SSA-888929: Missing Integrity Verification in LOGO! Soft Comfort

Publication Date 2017-12-18
Last Update 2017-12-18
Current Version V1.0
CVSS v3.0 Base Score 5.9

SUMMARY
The Update Center of LOGO! Soft Comfort lacks integrity verification on software packages downloaded via an unprotected communication channel. This could allow a remote attacker in a privileged network position to manipulate a software package during download.

Siemens provides SHA-256 checksums for all LOGO! Soft Comfort software packages to allow verification of legitimacy.

AFFECTED PRODUCTS
- LOGO! Soft Comfort: All versions < V8.2

DESCRIPTION
LOGO! Soft Comfort is an engineering software to configure and program LOGO! controllers. Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION
The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability Description (CVE-2017-12740)
The Update Center of LOGO! Soft Comfort lacks integrity verification on software packages downloaded via an unprotected communication channel. This could allow a remote attacker to manipulate the software package while performing a Man-in-the-Middle (MitM) attack.

CVSS Base Score 5.9

Mitigating Factors
In order to exploit the vulnerability, an attacker must be able to gain a privileged network position allowing him to capture and modify the affected system’s network communication.

SOLUTION
Siemens removed the Update Center from LOGO! Soft Comfort V8.2 [1] and provides SHA-256 checksums for all LOGO! Soft Comfort software packages via a secured channel (HTTPS) [2]. Siemens recommends verifying legitimacy by comparing the SHA-256 checksum of the downloaded software package with the SHA-256 checksum provided for the software package at [2].

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.
ACKNOWLEDGEMENTS
Siemens thanks the following for their support and efforts:

- Tobias Gebhardt for coordinated disclosure.

ADDITIONAL RESOURCES
[1] Software version 8.2 for LOGO! Soft Comfort can be obtained via:
   https://www.siemens.com/logo-update
[2] SHA-256 checksums for LOGO! Soft Comfort downloads can be obtained via:
   https://www.siemens.com/logo-update
   https://www.siemens.com/cert/operational-guidelines-industrial-security
[4] Information about Industrial Security by Siemens:
   https://www.siemens.com/industrialsecurity
[5] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
   https://www.siemens.com/cert/advisories

HISTORY DATA
V1.0 (2017-12-18): Publication Date

DISCLAIMER
See: https://www.siemens.com/terms_of_use