SSA-774850: Vulnerabilities in SIEMENS LOGO!8 devices

Publication Date: 2019-06-11
Last Update: 2020-02-10
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

Two vulnerabilities have been identified in SIEMENS LOGO!8 devices. The Session ID on the integrated webserver of LOGO!8 devices is not invalidated upon logout. The second vulnerability could allow an attacker with network access to port 10005/tcp to cause a Denial-of-Service condition by sending specifically crafted packages to the service.

Siemens provides a firmware update for the latest version of LOGO!8 devices. For older versions, the device needs to be upgraded (see table below).

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIEMENS LOGO!8 (incl. SIPLUS variants): 6ED1052-xyyxx-0BA8 FS:01 to FS:06 / Firmware version V1.80.xx and V1.81.xx	See Workarounds and Mitigations below or upgrade to a new version
SIEMENS LOGO!8 (incl. SIPLUS variants): 6ED1052-xyy08-0BA0 FS:01 / Firmware version < V1.82.02	Update to V1.82.02 or higher https://support.industry.siemens.com/cs/ww/en/view/109767410

WORKAROUNDS AND MITIGATIONS

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

- Protect network access to the device.
- As a general security measure Siemens strongly recommends to protect network access to the devices with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

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! 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-2019-6571

An attacker with network access to port 10005/tcp of the LOGO! device could cause a Denial-of-Service condition by sending specially crafted packets.

The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected service. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability compromises availability of the targeted system.

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

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2019-6584

The integrated webserver does not invalidate the Session ID upon user logout. An attacker that successfully extracted a valid Session ID is able to use it even after the user logs out.

The security vulnerability could be exploited by an attacker in a privileged network position who is able to read the communication between the affected device and the user or by an attacker who is able to obtain valid Session IDs through other means. The user must invoke a session to the affected device.

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

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-384: Session Fixation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Thomas Meesters from cirosec GmbH and Ruhr University of Bochum for coordinated disclosure of CVE-2019-6571

- Christian Siemers and Irakli Edjibia from Hochschule Augsburg for coordinated disclosure of CVE-2019-6584
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2019-06-11):	Publication Date
V1.1 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

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.