SSA-982399: Missing Authentication in TIM 1531 IRC Modules

Publication Date: 2018-12-11
Last Update: 2020-02-10
Current Version: V1.3
CVSS v3.1 Base Score: 10.0

SUMMARY

The latest update for TIM 1531 IRC fixes a vulnerability. The device was missing proper authentication when connecting on port 102/tcp, although configured.

An attacker needs to be able to connect to port 102/tcp of an affected device in order to exploit this vulnerability.

The vulnerability could allow an attacker to perform administrative operations.

Siemens has released updates for TIM 1531 IRC modules.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
TIM 1531 IRC (incl. SIPLUS NET variants): All versions < V2.0	Update to V2.0 https://support.industry.siemens.com/cs/ww/en/view/109762596

WORKAROUNDS AND MITIGATIONS

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

- Restrict access to port 102/tcp on TIM 1531 IRC to trusted IP addresses
- Update firmware to version V2.0 (and reload the TIM station from engineering)

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

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7, DNP3 and IEC 60870-5-101/104 with three RJ45 interfaces for communication via IP-based networks (WAN / LAN) and a RS 232/RS 485 interface for communication via classic WAN networks.

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-2018-13816

The device was missing proper authentication on port 102/tcp, although configured.

Successful exploitation requires an attacker to be able to send packets to port 102/tcp of the affected device. No user interaction and no user privileges are required to exploit the vulnerability.

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

CVSS v3.1 Base Score	10.0
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- 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 (2018-12-11):	Publication Date
V1.1 (2018-12-13):	Update not available, see mitigations
V1.2 (2018-12-17):	Description updated, update available
V1.3 (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.