SSA-941426: Multiple LLDP Vulnerabilities in Industrial Products

Publication Date: 2021-07-13
Last Update: 2021-08-10
Current Version: V1.1
CVSS v3.1 Base Score: 9.8

SUMMARY

There are multiple vulnerabilities in an underlying Link Layer Discovery Protocol (LLDP) third party library.

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
SIMATIC HMI Unified Comfort Panels: All versions < V17	Update to V17 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530
SIMATIC NET CP 1243-1 (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1243-8 IRC: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1542SP-1: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1542SP-1 IRC (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1543-1 (incl. SIPLUS variants): All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109800773
SIMATIC NET CP 1543SP-1 (incl. SIPLUS variants): All versions	See recommendations from section Workarounds and Mitigations
SIMATIC NET CP 1545-1: All versions	See recommendations from section Workarounds and Mitigations
SINUMERIK ONE MCP: All versions < V2.0.1	Update to V2.0.1 or later version Please contact your Siemens representative for information on how to obtain the update.
TIM 1531 IRC (incl. SIPLUS NET variants): All versions < V2.2	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798331

WORKAROUNDS AND MITIGATIONS

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

- Disable LLDP protocol support on Ethernet port. This will potentially disrupt the network visibility.

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

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

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.

The machine control panel SINUMERIK ONE MCP permits user-friendly operation of the machine functions at complex machining stations. It is suitable for machine-level operation of milling, turning, grinding and special machines.

The SIMATIC NET CP 1243-1 communication processor connects the S7-1200 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC NET CP 1243-8 IRC communication processor connects S7-1200 controllers via the SINAUT ST7 telecontrol protocol to a control center or master ST7 stations.

The SIMATIC NET CP 1543-1, CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communication processors connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC NET CP 1545-1 communication processor connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption. The communication processor protects S7-1500 stations against unauthorized access, as well as integrity and confidentiality of transmitted data.

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.

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-2015-8011

Buffer overflow in the lldp_decode function in daemon/protocols/lldp.c in lldpd before 0.8.0 allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via vectors involving large management addresses and TLV boundaries.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:T/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’)

Vulnerability CVE-2020-27827

Specially crafted LLDP packets can cause memory to be lost when allocating data to handle specific optional TLVs, potentially causing a denial of service.

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:T/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

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 (2021-07-13):	Publication Date
V1.1 (2021-08-10):	Added solution for SINUMERIK ONE MCP and SIMATIC NET CP 1543-1

TERMS OF USE