SSA-284673: Vulnerability in Industrial Products

Publication Date: 2018-01-18
Last Update: 2019-02-12
Current Version: V1.1
CVSS v3.0 Base Score: 6.5

SUMMARY

Several industrial devices are affected by a vulnerability that could allow an attacker to cause a Denial-of-Service condition via PROFINET DCP network packets under certain circumstances. Precondition for this scenario is a direct Layer 2 access to the affected products. PROFIBUS interfaces are not affected.

Siemens has released updates for several affected products, is working on updates for the remaining affected products and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Extension Unit 12" PROFINET: All versions < V01.01.01	Update to V01.01.01 https://support.industry.siemens.com/cs/de/en/view/109750351
Extension Unit 15" PROFINET: All versions < V01.01.01	Update to V01.01.01 https://support.industry.siemens.com/cs/de/en/view/109750351
Extension Unit 19" PROFINET: All versions < V01.01.01	Update to V01.01.01 https://support.industry.siemens.com/cs/de/en/view/109750351
Extension Unit 22" PROFINET: All versions < V01.01.01	Update to V01.01.01 https://support.industry.siemens.com/cs/de/en/view/109750351
SIMATIC CP 1242-7 GPRS V2: All versions < V2.1.82	Update to V2.1.82 https://support.industry.siemens.com/cs/ww/en/view/109749515
SIMATIC CP 1243-7 LTE/US: All versions < V2.1.82	Update to V2.1.82 https://support.industry.siemens.com/cs/ww/en/view/109749515
SIMATIC CP 1243-8: All versions < V2.1.82	Update to V2.1.82 https://support.industry.siemens.com/cs/ww/en/view/109749515
SIMATIC CP 1626: All versions < V1.1	Update to V1.1 https://support.industry.siemens.com/cs/ww/en/view/109763307

WORKAROUNDS AND MITIGATIONS

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

- Apply cell protection concept.
- Use VPN for protecting network communication between cells.
- Apply Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to run the devices in a protected IT environment, Siemens particularly 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

The SIMATIC CP 1242-7 and CP 1243-7 LTE communication processors connect the S7-1200 controller to Wide Area Networks (WAN). It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

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

SIMATIC CP 1626 enables SIMATIC PGs/PCs and PCs equipped with a PCI Express slot to be connected to PROFINET IO.

Extension Units PROFINET are available in different sizes to extend Simatic HMI Comfort PRO devices. All elements inside the extension unit are connected to PROFINET IO.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability (CVE-2017-2680)

Specially crafted PROFINET DCP broadcast packets could cause a Denial-of-Service condition of affected products on a local Ethernet segment (Layer 2). Human interaction is required to recover the systems. PROFIBUS interfaces are not affected.

CVSS v3.0 Base Score	6.5
CVSS Vector	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

ADDITIONAL INFORMATION

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 (2018-01-18): Publication Date
V1.1 (2019-02-12): Updated solution for SIMATIC CP 1626

TERMS OF USE