SSA-724606: Denial-of-Service Vulnerabilities in SIMATIC S7-1200 CPU Family

Publication Date: 2012-12-20
Last Update: 2020-02-10
Current Version: V1.3
CVSS v3.1 Base Score: 7.5

SUMMARY

Siemens SIMATIC S7-1200 PLCs, version 2 and higher, allow device management over TCP port 102 (ISO-TSAP) and retrieving status information over UDP port 161 (SNMP). It is possible to cause the device to go into defect mode by sending specially crafted packets to these ports.

Siemens addresses these issues with the newest product release.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.0.0	Update to V4.0.0 http://support.automation.siemens.com/WW/view/en/86567043

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

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

Products of the SIMATIC S7-1200 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

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-2013-2780

Specially crafted packets sent on port 161/udp (SNMP) cause the device to go into defect mode.

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-20: Improper Input Validation

Vulnerability CVE-2013-0700

Specially crafted packets sent on port 102/tcp (ISO-TSAP) cause the device to go into defect mode. Further research has identified multiple instances of this vulnerability.

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-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Prof. Dr. Hartmut Pohl from softScheck GmbH for coordinated disclosure of CVE-2013-2780
- Arne Vidström from Swedish Defence Research Agency (FOI) for coordinated disclosure of CVE-2013-0700
- 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 (2012-12-20):	Publication Date
V1.1 (2013-02-13):	Closer analyses by Arne Vidström showed different ways to exploit CVE-2013-0700
V1.2 (2014-03-20):	Added information about PLC version V4
V1.3 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE