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

Publication Date 2012-12-20
Last Update 2012-12-20
Current Version V1.0
CVSS Overall Score 7.0

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 is preparing a solution for these issues that will be available in the next scheduled product update. Customers will be advised when this release is available.

AFFECTED PRODUCTS

Siemens SIMATIC S7-1200 V2.x and V3.x

DESCRIPTION

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

When specially crafted packets are received on the devices' Ethernet network interfaces, the device may go into the stop/defect state. The device needs to be manually reset to continue with normal operation. Attackers could use these vulnerabilities to perform a Denial-of-Service attack.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://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 1

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

CVSS Base Score 7.8
CVSS Temporal Score 7.0
CVSS Overall Score 7.0 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:POC/RL:U/RC:C)

Vulnerability 2

Specially crafted packets sent on TCP port 102 (ISO-TSAP) cause the device to go into defect mode.

CVSS Base Score 7.8
CVSS Temporal Score 7.0
CVSS Overall Score 7.0 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:POC/RL:U/RC:C)

Mitigating factors:

The attacker must have network access to the affected devices. For vulnerability 1 and vulnerability 2 the ports must be accessible. Siemens recommends operating the devices only within trusted networks [2].

SOLUTION

Siemens is preparing a solution for these issues that will be available in the next scheduled product update. Customers will be advised and this advisory will be updated when the new release is available.

The affected software components are implemented under the assumption of running in a protected network environment. Siemens strongly recommends to protect systems according to recommended security practices in [3] and to configure the environment according to operational guidelines [1].

ACKNOWLEDGEMENT

Siemens thanks the following researchers for informing us about the vulnerabilities in a coordinated manner:

- Vulnerability 1: Prof. Dr. Hartmut Pohl, softScheck GmbH
- Vulnerability 2: Arne Vidstrom, Swedish Defence Research Agency (FOI)

ADDITIONAL RESOURCES

1. An overview of the operational guidelines for Industrial Security (with the cell protection concept):
   http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf
2. Information about Industrial Security by Siemens:
   http://www.siemens.com/industrialsecurity
3. Recommended security practices by US-CERT:
   http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html
4. For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
   http://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2012-12-20): Publication Date

DISCLAIMER