SSA-453276: Denial-of-Service Vulnerability in SIMATIC NET PC-Software

Publication Date 2016-07-22
Last Update 2016-07-22
Current Version V1.0
CVSS v3.0 Base Score 5.3

SUMMARY

The latest version of SIMATIC NET PC-Software fixes a vulnerability that could allow remote attackers to cause a Denial-Of-Service on several OPC-UA ports under certain conditions.

AFFECTED PRODUCTS

SIMATIC NET PC-Software: All versions < V13 SP2

DESCRIPTION

SIMATIC NET PC-Software is required for communication between controllers (PLCs) and PC based solutions (HMIs).

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3 (CVSS v3.0) (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 assessed by the customer to accomplish final scoring.

Vulnerability Description (CVE-2016-5874)

Specially crafted packets sent to several ports (55101/tcp – 55105/tcp, 4845/tcp, 4847/tcp – 4850/tcp) could cause a denial-of-service of the OPC UA service. A manual restart of the service is required to recover the system.

CVSS Base Score 5.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

Mitigating Factors

The attacker must have network access to the affected devices. Siemens recommends operating SIMATIC NET PC-Software only within trusted networks [2].

SOLUTION

Siemens provides SIMATIC NET PC-Software V13 SP2 [1], which fixes the vulnerability, and recommends users to upgrade to the new version.

If OPC-UA is not required, Siemens recommends deactivating these in the communication settings according to the information in the respective product manual.

As a general security measure Siemens strongly recommends to protect network access to SIMATIC NET PC-Software services with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [2] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks Sergey Temnikov and Vladimir Dashchenko, Critical Infrastructure Defence Team, Kaspersky Lab for coordinated disclosure of the vulnerabilities.

ADDITIONAL RESOURCES

[1] SIMATIC NET PC-Software V13 SP2 can be obtained by contacting your local Siemens representative or customer support.

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept): https://www.siemens.com/cert/operational-guidelines-industrial-security

[3] Information about Industrial Security by Siemens: https://www.siemens.com/industrialsecurity

[4] 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 (2016-07-22): Publication Date

DISCLAIMER