SSA- 934525: Vulnerability in SINUMERIK Integrate

Publication Date 2017-03-01
Last Update 2017-03-01
Current Version V1.0
CVSS v3.0 Base Score 7.4

SUMMARY

The latest updates for SINUMERIK Integrate and SINUMERIK Operate fix a vulnerability that could under certain conditions allow attackers in a privileged network position to capture and modify network traffic protected with TLS.

AFFECTED PRODUCTS

- SINUMERIK Integrate Access MyMachine /Ethernet with
  - AMM Service Engineer Client (ActiveX): All versions
- SINUMERIK Integrate Access MyMachine /Ethernet and Analyze MyCondition with
  - SINUMERIK Integrate Operate Client:
    - All versions between 2.0.3.00.016 (including) and 2.0.6 (excluding)
    - All versions between 3.0.4.00.032 (including) and 3.0.6 (excluding)

  Affected SINUMERIK Integrate Operate clients are included in the following SINUMERIK Operate releases:
    - All versions between V4.5 SP6 (including) and V4.5 SP6 Hotfix 8 (excluding)
    - All versions between V4.7 SP2 Hotfix 1(including) and V4.7 SP4 (excluding)

DESCRIPTION

SINUMERIK Integrate product suite facilitates simple networking of machine tools in the IT of the production landscape.

SINUMERIK Operate is a standard Human-Machine-Interface system for SINUMERIK numerical controls.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (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-2017-2685)

A vulnerability could allow an attacker to read and manipulate data in TLS sessions while performing a man-in-the-middle (MITM) attack. Clients are only affected if HTTPs is used.

CVSS Base Score 7.4
CVSS Vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

SOLUTION

Siemens provides the following updates for affected SINUMERIK Integrate and SINUMERIK Operate versions:

- SINUMERIK Integrate Access MyMachine /Ethernet and Analyze MyCondition with
  - SINUMERIK Operate V4.7:
    - Update to SINUMERIK Operate to V4.7 SP4 [1], or
    - Update SINUMERIK Integrate Operate Client to V3.0.6 [1]
  - SINUMERIK Operate V4.5:
    - Update to SINUMERIK Operate to V4.5 SP6 Hotfix 8 [1], or
    - Update SINUMERIK Integrate Operate Client to V2.0.6 [1]
- SINUMERIK Integrate Access MyMachine /Ethernet with
  - AMM Service Engineer Client (ActiveX): Replace with AMM Service Client V4.1.0.5 [1] / Replacement will be automatically installed when connecting to SINUMERIK Integrate V4.1 SP5 or newer

As a general security measure Siemens strongly recommends to configure the environment according to our operational guidelines [2] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] The update can be obtained from your local service organization. If assistance in identifying your local service organization is required, please contact a local Siemens hotline center: https://w3.siemens.com/aspa_app/.

[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 (2017-03-01): Publication Date

DISCLAIMER