SSA-729965: TLS Certificate Validation Vulnerability in SINUMERIK Integrate Operate Client

Publication Date: 2021-07-13
Last Update: 2021-07-13
Current Version: V1.0
CVSS v3.1 Base Score: 7.4

SUMMARY

The latest update for SINUMERIK Integrate Operate Client fixes a vulnerability that could allow an attacker to spoof any SSL server certificate and conduct man-in-the-middle attacks.

Siemens is preparing updates and recommends specific countermeasures for products where updates are not, or not yet available

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINUMERIK Analyse MyCondition: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Analyze MyPerformance: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Analyze MyPerformance /OEE-Monitor: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Analyze MyPerformance /OEE-Tuning: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Integrate Client 02: All versions >= V02.00.12 < 02.00.18	Update to V02.00.18 Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Integrate Client 03: All versions >= V03.00.12 < 03.00.18	Update to V03.00.18 Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Integrate Client 04: V04.00.02 and all versions >= V04.00.15 < 04.00.18	Update to V04.00.18 Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Integrate for Production 4.1: All versions < V4.1 SP10 HF3	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Integrate for Production 5.1: V5.1	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.

SINUMERIK Manage MyMachines: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Manage MyMachines /Remote: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Manage MyMachines /Spindel Monitor: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Manage MyPrograms: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Manage MyResources /Programs: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Manage MyResources /Tools: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Manage MyTools: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Operate V4.8: All versions < V4.8 SP8	Update SINUMERIK Operate to V4.8 SP8 or update included SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Operate V4.93: All versions < V4.93 HF7	Update SINUMERIK Operate to V4.93 HF7 or update included SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Operate V4.94: All versions < V4.94 HF5	Update SINUMERIK Operate to V4.94 HF5 or update included SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.
SINUMERIK Optimize MyProgramming /NX-Cam Editor: All versions	Update SINUMERIK Integrate Client Please contact your Siemens representative for information on how to obtain the update.

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific mitigations or workarounds. Please follow General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

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

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

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-2021-31892

Due to an error in a third-party dependency the ssl flags used for setting up a TLS connection to a server are overwitten with wrong settings. This results in a missing validation of the server certificate and thus in a possible TLS MITM szenario.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

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 (2021-07-13):	Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.