SSA-285795: Denial of Service in OPC-UA in Industrial Products

Publication Date: 2022-05-10
Last Update: 2022-05-10
Current Version: V1.0
CVSS v3.1 Base Score: 6.5

SUMMARY

Vulnerability in the underlying third party component OPC UA ANSIC Stack (also called Legacy C-Stack) affects several industrial products. The vulnerability could cause a crash of the component that includes the vulnerable part of the stack.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC NET PC Software V14: All versions < V14 SP1 Update 14	Update to V14 SP1 Update 14 or later version https://support.industry.siemens.com/cs/ww/en/view/109807351/ See further recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V15: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V16: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC NET PC Software V17: All versions < V17 SP1	Update to V17 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109808270/ See further recommendations from section Workarounds and Mitigations
SITOP Manager: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
TeleControl Server Basic V3: All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Do not use OPC client feature to connect via untrusted networks or to untrusted OPC-UA communication partners
- Use VPN for protecting network communication between cells

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

Please follow the General Security Recommendations.

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

SIMATIC NET PC software is a software product that is sold separately and implements the communications product from SIMATIC NET.

SITOP Manager is a tool for commissioning, engineering and monitoring of SITOP power supplies with communication capabilities.

TeleControl Server Basic allows remote monitoring and control of plants.

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-2021-45117

The OPC UA ANSIC Stack (also called Legacy C-Stack) was reported to crash when an unexpected OPC UA Response message status code was accessed via the synchronous Client API. The vulnerability was found in generated code of the OPC Foundation C-Stack. An unexpected status code in response message will dereference Null pointer leading to crash, ping of death (PoD). This affects a client, but it might also affect a server when it uses OpcUa_ClientApi_RegisterServer (e.g. register at LDS). A specially crafted UA server, or Man in the Middle attacker, can cause the OPC UA application to crash by sending uncertain status code in response message.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

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 (2022-05-10): Publication Date

TERMS OF USE