BECKHOFF

Advisory 2017-001: ADS is only designed for use in protected environments

Publication Date	03/13/2017
Last Update	12/03/2019
Current Version	1.4
Relevance	Medium
Related CVE	CVE-2017-16726, CVE-2019-16871

Summary

ADS is only advised to be used in protected environments, and as such does not provide security properties. Attackers can eavesdrop, manipulate and forge arbitrary packets as in any other cleartext protocol. In case ADS access is possible, various system related services can be used.

Appearance

- TwinCAT 2 / 3

Description

Beckhoff TwinCAT supports communication over ADS. ADS is a protocol for industrial automation in protected environments [1]. ADS has not been designed to achieve security purposes and therefore does not include any encryption algorithms because of their negative effect on performance and throughput.

- An attacker can forge arbirtrary ADS packets when legitimate ADS traffic is observable.
- An attacker, who has access via ADS could make use of various local services

Solution

Use ADS Protocol only in protected environments, where security measures are not required and no attack is possible. In case all ADS applications are running on the same system, Beckhoff recommends to block ADS via firewall.
In case of distributed applications, we recommend to make use of other protocols (e.g. ADS over IPSec, ADS-over-MQTT, OPC-UA) or Secure ADS, which is available since TwinCAT 3.1 Build 4024.0. This could be used to transfer ADS messages over an encrypted connection. Optionally, the non-encrypted ADS could be disabled and uni-directional connections could be configured. It is still valid that who ever has access via ADS could use various local services like described above.

Acknowledgement

Beckhoff Automation thanks for their support and efforts:

- Peter Schwanke, who is a student at FH Aachen, for coordinated disclosure.
- Yury Serdyuk from Kaspersky Lab for coordinated disclosure.

Reporting vulnerabilities

Beckhoff Automation welcomes responsibly coordinated reports of vulnerabilities and Beckhoff will collaborate with reporting parties to fix vulnerabilities or mitigate threats.

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20, 33415 Verl, Germany
Phone: +49 (0) 52 46/9 63 - 0
E-Mail: product-secincident@beckhoff.com
www.beckhoff.com

Additional Resources

[1] A general guideline for Beckhoff IPC Security:
http://download.beckhoff.com/download/Document/IndustPC/IPC_Security_EN.pdf

History

V 1.0	03/13/2017	Publication
V 1.1	07/02/2018	Added CVE
V 1.2	01/29/2019	Added more precise information
V 1.3	10/10/2019	Added note about Secure ADS since TwinCAT 3.1 Build 4024.0
V 1.4	12/03/2019	Added CVE-2019-16871 as reference

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20, 33415 Verl, Germany
Phone: +49 (0) 52 46/9 63 - 0
E-Mail: product-secincident@beckhoff.com
www.beckhoff.com