Advisory 2014-002: ADS communication port allows password bruteforce

Publication Date	11/17/2014
Last Update	02/24/2015
Current Version	V 1.1
Relevance	Medium

Summary

Beckhoff TwinCAT Products are delivered with ADS technology. An attacker may misuse this protocol to guess passwords.

Appearance

- All TwinCAT Compontents featuring ADS communication

Description

The TwinCAT Automation Device Specification (ADS) is the medium-independent protocol for the reading and writing of data and for instruction transmission within TwinCAT. 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. Attackers may use this protocol to rapidly probe a large number of user/password combinations.

Precondition of the exploitation is the ability to communicate ADS data with the affected system.

Solution

This can either be solved by:

- Restriction of ADS communication to trusted networks only.
- The IPC Security Manual [1] provides suggestions/recommendations for secure usage of ADS communication.

Reporting vulnerabilities

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

Additional Resources

[1] IPC Security Manual:
http://download.beckhoff.com/download/Document/IndustPC/IPC_Security_EN.pdf

History

V 1.0	11/17/2014	Publication
V 1.1	02/24/2015	Revision

Beckhoff Automation GmbH
Eiserstr. 5, 33415 Verl, Germany
Phone: +49 (0) 52 46/9 63 - 0
E-Mail: product-secincident@beckhoff.com
www.beckhoff.com