Advisory 2017-002: Add Route using "Encrypted Password" bases on fixed key

Publication Date	03/13/2017
Last Update	07/02/2018
Current Version	1.1
Relevance	Medium
Related CVE	CVE-2017-16718

Summary

Adding routes in ADS router supports encryption of credentials. This encryption bases on a fixed key. Attackers could extract the fixed key in order to decrypt those credentials. Adding routes only locally prevents exposure of the credentials.

Appearance

- All TwinCAT 3 Components featuring ADS remote route creation

Description

Beckhoff TwinCAT 3 supports communication over ADS. ADS is a protocol for industrial automation in protected environments [1]. This protocol uses user configured routes, that can be edited remotely via ADS. This special command supports encrypted authentication with username/password. The encryption uses a fixed key, that could be extracted by an attacker.

Precondition of the exploitation of this weakness is network access at the moment a route is added.

Solution

By adding the static routes only locally, no credentials will be transferred via network.

https://infosys.beckhoff.de/content/1033/tc3_system/html/tcsysmgr_systemnode_subnodes_routes.htm

Acknowledgement

Beckhoff Automation thanks for his support and efforts:

▪ Peter Schwanke, who is a student at FH Aachen, 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.

Additional Resources

[1] A general guideline for Beckhoff IPC Security:
http://download.beckhoff.com/download/Document/product-security/ipc_security_en.pdf

History

V 1.0	03/13/2017	Publication
V 1.1	07/02/2018	Added CVE

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