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

Publication Date	03/13/2017
Last Update	12/18/2023
Current Version	1.3
Related CVE	CVE-2017-16718
CVSS 3.0	5.9 Medium (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Weakness Enumerator	CWE-321 Use of Hard-coded Cryptographic Key

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, except TwinCAT/BSD based products

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.

Please note: TwinCAT/BSD based products have been released only after this advisory was published first time. They come with default settings where the vulnerable ADS communication is blocked. Secure ADS is used as a default replacement there which guards the credentials with a TLS encryption.

Solution

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

https://infosys.beckhoff.com/content/1033/tc3_system/818866059.html

Alternative is to block plain ADS and use Secure ADS only as described with the following document:
https://download.beckhoff.com/download/document/automation/twincat3/Secure_ADS_EN.pdf
All recent products from Beckhoff support it.

Please note: Because TwinCAT/BSD based products come with default settings which do forbid plain ADS communication but allow Secure ADS communication these settings shall not be changed for security reasons.

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

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
V 1.2	12/11/2023	Added exception for TwinCAT/BSD Added the use of Secure ADS as an alternative.
V 1.3	12/18/2023	Corrected a hyperlink

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