Advisory 2019-04: ADS Discovery Service Shutdown by special UDP packet

Publication Date	07/08/2019
Last Update	07/08/2019
Current Version	1.0
Relevance	High
Related CVE	CVE-2019-5636

Summary

When a TwinCAT Runtime receives an UDP packet with a data length of 0 byte, the ADS Discovery Service shuts down. TwinCAT devices are still performing as normal.

Appearance

All TwinCAT versions equal or below

- TwinCAT 2 Build 2304
- TwinCAT 3.1 Build 4024.0

Description

ADS Discovery is performed via UDP. It provides the capability to discover TwinCAT devices within a network. During operation, this service is not used since routes have already been established and there is no need to discover additional devices.

When a UDP packet with a data length of 0 byte is received on the UDP discovery port, the service shuts down.

Establishing new ADS routes by using the hostname / IP address is still possible but the Broadcast-Search of TwinCAT will not show the device anymore.

Mitigation

Beckhoff will provide new versions of TwinCAT. The UDP Port 48899 could be blocked in perimeter firewall to prevent such UDP packets from untrusted networks. Please keep in mind that ADS should only be used in trustfull environments, cmp. Security Advisory 2017-01. [1]

Acknowledgement

Beckhoff Automation thanks Andreas Galauner from Rapid7 for support and efforts within coordinated disclousure.

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-securityincident@beckhoff.com
www.beckhoff.com

Additional Resources

[1] Advisory 2017-001: ADS is only designed for use in protected environments.
https://download.beckhoff.com/download/Document/product-security/Advisories/advisory-2017-001.pdf

History

V 1.0	07/08/2019	Publication

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