Advisory 2018-002: Updates for OPC-UA components (Several Vulnerabilities)

Publication Date	05/18/2018
Last Update	-
Current Version	1.0
Relevance	High
Related CVE	CVE-2017-17443, CVE-2017-12069

Summary

Kaspersky Lab published a report about vulnerabilities in OPC UA software stacks [2]. Denial of Service and access to arbitary network ressources are potential attacks.

Updates for Beckhoff components are available.

Appearance

- TF6100 | TwinCAT OPC-UA 4.x < Version 4.1.3.0 and 3.x < Version 3.3.17.0
- TS6100-00300 | TwinCAT OPC UA Server CE < Version 3.3.17.0
- TS6100 | TwinCAT OPC UA Server < Version 3.3.17.0
- TF6720 | TwinCAT Data Agent < Version 1.1.10.0
- IPC Diagnostics < Version 1.8.4

Description

Beckhoff OPC-UA components base on the generic stacks of the OPC Foundation.

OPC Foundation adressed the findings and reported in the following advisories:

CVE-2017-12069

This security update resolves a vulnerability in the OPC UA .NET Sample Code and older versions of the Local Discovery Services (LDS) binaries which can be downloaded from the OPC Foundation website. The vulnerability can allow remote attacker to trick the .NET libraries used by the LDS and OPC UA Servers into accessing network resources chosen by the attacker. [4]

CVE-2017-17443

This security update to resolves multiple vulnerabilities that allow an attacker to trigger a crash by placing invalid data into the configuration file. This vulnerability requires an attacker with access to the file system where the configuration file is stored; however, if the configuration file is altered the LDS will be unavailable until it is repaired. [3]

Solution

Upgrade to a fixed Version

- TF6100 | TwinCAT OPC-UA 4x to Version 4.1.3.0 or higher and 3.x to Version 3.3.17.0 or higher
- TS6100-00300 | TwinCAT OPC UA Server CE to Version 3.3.17.0 or higher
- TS6100 | TwinCAT OPC UA Server to Version 3.3.17.0 or higher
- TF6720 | TwinCAT Data Agent to Version 1.1.10.0 or higher
- Update IPC Diagnostics to Version 1.8.4 or higher

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

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

[2] Pavel Cheremushkin and Sergey Temnikov. *OPC UA security analysis.*
http://download.beckhoff.com/download/Document/product-security/ipc_security_en.pdf. 2018

[3] OPF Foundation. *Security Update for the Local Discovery Server (LDS).* https://opcfoundation-onlineapplications.org/faq/SecurityBulletins/OPC_Foundation_Security_Bulletin_CVE-2017-17443.pdf. 2017

[4] OPF Foundation. *Security Update for the OPC UA .NET Sample Code.* https://opcfoundation-onlineapplications.org/faq/SecurityBulletins/OPC_Foundation_Security_Bulletin_CVE-2017-12069.pdf. 2017

History

V 1.0	05/18/2018	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