Advisory 2015-001: Potential misuse of IPC Diagnostics < 1.8 UPnP backend

Publication Date	21/05/2015
Last Update	03/06/2015
Current Version	V 1.1
Relevance	Medium

Summary

Beckhoff IPC diagnostics offer options during operation, with integrated access to the existing hardware and software components. An attacker may misuse the UPnP backend of this tool CVE-2015-4051 [2].

Appearance

- All Images containing IPC Diagnostics < version 1.8

Description

An unauthenticated attacker may misuse all functions available through the IPC Diagnostics Website. This may affect the availability through reboot and shutdown functionalities as also the integrity of the IPC through creation of users.

Precondition of the exploitation of this weakness is network access to affected systems.

Solution

- An updated version 1.8 of the IPC Diagnostics is available at ftp://ftp.beckhoff.com/Software/embPC-Control/Solution/IPC-Diagnostics/ enforcing authentication for each functionality.
- Restriction of the network access is proposed for IPCs [1]

As new images are released integrating version 1.8 or later they will be listed in updates of this advisory:

- No image released yet, please use the IPC Diagnostics Setup

Acknowledgement

Beckhoff Automation thanks for his support and efforts:

- Frank Lycops from the Security Factory 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

References

[1] Beckhoff Automation GmbH & Co. KG. A general guideline for Beckhoff IPC Security. URL http://download.beckhoff.com/download/Document/IndustPC/IPC_Security_EN.pdf.

[2] National Institute of Standards and Technology. CVE-2015-4051 in National Vulnerability Database, 2015. URL https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4051.

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

History

V 1.0	21/05/2015	Publication
V 1.1	03/06/2015	Revision and introduction of the image-list
V 1.2	17/10/2015	Added reference to CVE number

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