BECKHOFF

Advisory 2019-06: CE Remote Display behaves incorrectly with wrong credentials

Publication Date	03/09/2019
Last Update	10/10/2019
Current Version	1.2
Relevance	High

Summary

The CE Remote Display under Windows CE and Windows Embedded Compact 7 does not behave correctly with incorrect login information. This leads to access even with incorrect credentials if a modified version of the CE Remote Host Client is used.

Appearance

All standard Beckhoff Windows CE and Windows Embedded Compact 7 images for the following devices:

Embedded PC	IPC Motherboard	CE6 / WEC7	Version	TwinCAT Version / Build	Image Name
CX50x0	CBx053	CE6.0	3.56	TC2 Build 2304	CBx053_CE600_HPS_v356_TC211R3_B2304
CX50x0	CBx053	CE6.0	4.06a	TC3.1 Build 4022.29	CBx053_CE600_HPS_v406a_TC31_B4022.29
	CB3052, CB3054	CE6.0	3.56	TC2 Build 2304	CB3052_CB3054_CE600_HPS_v356_TC211R3_B2304
	CB3052, CB3054	CE6.0	4.06a	TC3.1 Build 4022.29	CB3052_CB3054_CE600_HPS_v406a_TC31_B4022.29
CX20x0	CBx055, CBx056	WEC7	5.04	TC2 Build 2304	CBx055_CBx056_WEC7_HPS_v504_TC211R3_B2304
CX20x0	CBx055, CBx056	WEC7	6.06a	TC3.1 Build 4022.29	CBx055_CBx056_WEC7_HPS_v606a_TC31_B4022.29
CX51x0	CBxx63	WEC7	5.04	TC2 Build 2304	CBxx63_WEC7_HPS_v504_TC211R3_B2304
CX51x0	CBxx63	WEC7	6.06a	TC3.1 Build 4022.29	CBxx63_WEC7_HPS_v606a_TC31_B4022.29
CX9020	CB3011	WEC7	5.04	TC2 Build 2304	CX9020_CB3011_WEC7_HPS_v504_TC211R3_B2304
CX9020	CX9020	WEC7	6.04j	TC3.1 Build 4022.29	CX9020_CB3011_WEC7_HPS_v604j_TC31_B4022.25
CX8000	CX8000	CE6	3.56	TC2 Build 2304	CX8000_CE600_LF_v356_TC211R3_B2304
CX8190	CX8190	WEC7	6.06a	TC3.1 Build 4022.29	CX8100_WEC7_LF_v606a_TC31_B4022.29

If the Version number on the device is higher than mentioned here, the devices have already a fixed image.

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

Description

By default, the CE Remote Display is disabled in Beckhoff images since the following versions:

Embedded PC	IPC Motherboard	CE6 / WEC7	Version	TwinCAT Version / Build	Image Name
CX50x0	CBx053	CE6.0	3.54	TC2 Build 2245	CBx053_CE600_HPS_v354_TC211R3_B2245
CX50x0	CBx053	CE6.0	4.02	TC3.1 Build 4016.6	CBx053_CE600_HPS_v402_TC31_B4016.6
	CB3052, CB3054	CE6.0	3.54c	TC2 Build 2249	CB3052_CB3054_CE600_HPS_v354c_TC211R3_B2249
	CB3052, CB3054	CE6.0	4.02	TC3.1 Build 4016.6	CB3052_CB3054_CE600_HPS_v402_TC31_B4016.6
CX20x0	CBx055, CBx056	WEC7	5.02a	TC2 Build 2247	CBx055_CBx056_WEC7_HPS_v502a_TC211R3_B2247
CX20x0	CBx055, CBx056	WEC7	6.02	TC3.1 Build 4016.6	CBx055_CBx056_WEC7_HPS_v602_TC31_B4016.6
CX51x0	CBxx63	WEC7	5.02g	TC2 Build 2256	CBxx63_WEC7_HPS_v502g_TC211R3_B2256
CX51x0	CBxx63	WEC7	6.02l	TC3.1 Build 4018.33	CBxx63_WEC7_HPS_v602l_TC31_B4018.33
CX9020	CX9020	WEC7	5.02b	TC2 Build 2249	CX9020_CB3011_WEC7_HPS_v502b_TC211R3_B2249
CX9020	CX9020	WEC7	6.02	TC3.1 Build 4016.6	CX9020_CB3011_WEC7_HPS_v602_TC31_B4016.6
CX8000	CX8000	CE6.0	3.54b	TC2 Build 2248	CX8000_CE600_LF_v354b_TC211R3_B2248
CX8190	CX8190	WEC7	6.04e	TC3.1 Build 4022.14	CX8100_WEC7_LF_v604e_TC31_B4022.14

The CE Remote Display can be active in custom or previously provided images or when the default values are changed manually. CE Remote Display uses an unencrypted protocol. Do not use it in untrusted network environments. The CE Remote Display Tool does not close the incoming connection on the Windows CE side if the credentials are incorrect. The original CE Remote Host client terminates this connection. A modified version establishes a connection without correct credentials.

Solution

Beckhoff provides updated images for the mentioned devices.

The images could be obtained via https://download.beckhoff.com/download/software/embPC-Control followed by the device type.

Mitigation

In case of the solution is not applicable, please consider one the following mitigations:

- Disable the CE Remote Display service on the devices.
- Establish access control via for example a perimeter firewall

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

Acknowledgement

Beckhoff Automation thanks

- Chen Jie from NSFOCUS for support and efforts within coordinated disclousure.
- Tijl Deneut from University Howest for support and additional information.

Reporting vulnerabilities

Beckhoff Automation welcomes responsibly coordinated reports of vulnerabilities and Beckhoff will collaborate with reporting parties to fix vulnerabilities or mitigate threats.

History

V 1.0	03/09/2019	Publication
V 1.1	04/09/2019	Table of images updated
V 1.2	10/10/2019	Added Tijl Denaut to Acknowledge section Added Information about availability of new images – see Solution

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