Advisory 2014-001: Potential misuse of several administrative services

Publication Date	11/17/2014
Last Update	02/24/2015
Current Version	V 1.1
Relevance	Medium

Summary

Beckhoff Embedded PC Images by default provide tools that help to administer the EPC. An attacker may misuse these tools.

Appearance

- All Beckhoff Embedded PC Images creation date < 10/22/2014

Description

Beckhoff Images (creation date < 10/22/2014) for Embedded PCs (EPCs) are delivered with the Windows CE Remote Configuration Tool reachable at the web server path /remoteadmin, enabled CE Remote Display service, and enabled telnet service. Use of these services is recommended only in trusted networks. If used without proper protection an attacker may misuse those services to gain unauthorized access to systems or read and manipulate transmitted information, especially passwords.

Precondition of the exploitation of those services is that the attacker has access to the services at the corresponding network ports (TCP 80/987/23). This implies that the services are running.

Solution

This can either be solved by:

- Updating to images build >= 10/22/2014 solves this by disabling the services by default
- The configuration of the web server pathes can be found in the Windows registry at the path “HKEY_LOCAL_MACHINE\COMM\HTTPD\VROOTS\”. To disable the Windows CE Remote Configuration Tool delete the subtree “/remoteadmin”.
- Disable startup of CE Remote Display service (cerdisp.exe) with deleting the registry key containing the “CeRDisp.exe“ [-HKEY_LOCAL_MACHINE\init\Launch90]
- Disable telnet by setting the registry key [HKEY_LOCAL_MACHINE\Services\TELNETD\Flags] to dword:4
- The IPC Security Manual [1] provides information for securing the environment of an EPC.

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] IPC Security Manual:
http://download.beckhoff.com/download/Document/IndustPC/IPC_Security_EN.pdf

History

V 1.0	11/17/2014	Publication
V 1.1	02/24/2015	Revision