Security Advisory
WannaCry

1 Advisory Information

Advisory ID: BOSCH-SA-684353
Published: 29 May 2017
Last Updated: 29 May 2017

2 Summary

Industrial PC and embedded PC devices with Windows operating systems Windows XP, Windows 7 and Windows 10 and an operating system version older than March 2017, are susceptible to remote code execution via SMB [1].
Currently, “WannaCry” ransomware exploits this weakness in order to distribute malware and to encrypt data of affected systems.

3 Affected Products

Products of the following Rexroth device families are potentially at risk

- IndraControl VPB
- IndraControl VPP
- IndraControl VSP
- IndraControl VEP
- IndraControl VEH

if they are using the following operating system firmware:

Windows 10 IoT Enterprise LTSB 2015
- R911375308 FWA-VP3***-W10-01VRS-A0
- R911376378 FWA-VP4***-W10-01VRS-A0
- R911375475 FWA-VEP*06-W10-01VRS-D0

Windows Embedded Standard 7
- R911172607 FWA-VP3***-W7*-01VRS-A0-OEM
- R911172608 FWA-VP3***-W7*-01VRS-A0-OEM A1
- R911338555 FWA-VP3***-W7*-01VRS-A0-OEM A1 32
- R911376435 FWA-VP4***-W7*-01VRS-A0-OEM
- R911377579 FWA-VP4***-W7*-01VRS-A0-OEM A1
- R911377580 FWA-VP4***-W7*-01VRS-A0-OEM A1 32
- R911337389 FWA-VEP*05-W7*-01VRS-D0-A* 32
- R911370518 FWA-VEP*06-W7*-01VRS-D0-A4 32

Windows 7 Ultimate

- R911338554 FWA-VP3***-W7U-01VRS-A0-OEM A1
- R911346128 FWA-VP3***-W7U-01VRS-A0-OEM A1 32
- R911377581 FWA-VP4***-W7U-01VRS-A0-OEM A1
- R911377582 FWA-VP4***-W7U-01VRS-A0-OEM A1 32

Windows XP

- R911172447 FWA-VS3VP3-WXP-03VRS-A0-OEM
- R911172448 FWA-VS3VP3-WXP-03VRS-A0-OEM A1

Windows XPe

- R911334113 FWA-VEP*04-XPE-01VRS-D0-A*
- R911324056 FWA-VEP*04-XPE-01VRS-D0-C*
- R911172171 FWA-VEH*02-XPE-01VRS-D0-A*
- R911337390 FWA-VEP*05-XPE-01VRS-D0-A*

As well as the screw control CS351 variant 0608PE1977 with integrated Windows XP based plug-in card.

4 Solution

If an HMI device is operated locally, without a network connection, no additional measures are necessary with regard to the spread of WannaCry.
In case of operation of HMI networking devices, installation of the safety patches provided by Microsoft in March 2017 is recommended:

Windows 10

- KB4012606

Windows 7 32 bit and 64 bit

- KB4012212

Windows XP and XPe

- KB4012598

If a customization of the operating system's settings is not possible in a net-worked environment and the patches specified above cannot be installed due to compatibility reasons, the system has to be separated from the network by external measures (e.g. by blocking the communication via the ports relevant for WannaCry, ports 135, 137-139 and 445, by means of hardware firewall).

4.1 General safety measures for networked plants

In order to allow for the continuous, trouble-free operation of production lines, we recommend complying with some basic principles:

- Reliable separation of control and plant networks from other networks by means of an appropriate network infrastructure.
- In the plant network, only the programs and services required for the pro-duction should be utilized and permitted.
- No use of mobile data carriers (USB sticks) in the plant network.

- Avoid the use of Office and mail programs, for example, in the plant network.
- Check and secure PCs by means of an up-to-date virus scanner on a regular basis.

5 Vulnerability Details

The devices may get infected with the above-mentioned ransomware by the execution of infected data (mail attachments, active Office files, executable programs) or also when used in a network with other infected devices.

6 Additional Resources

[1] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

For further questions and for support in the implementation of safety measures, contact our service staff at**:** **+49 9352 405060**.

7 Revision History

29 May 2017: Initial Publication