

Date:	18.04.2018
Subject:	WannaCry Ransomware Analysis for Windows CE 5.0/ CE 6.0/ EC 7.0
Severity rating:	Medium
Product:	XC/XV and similar devices

General Information

WannaCry is a self-propagating ransomware capable of encrypting files in affected systems. It appends affected encrypted files with the .WCRY extension and demands a fee for decryption.

WannaCry, unlike most ransomware, is not distributed via an email spam campaign. It is spread by taking advantage of a vulnerability in Microsoft's Server Message Block (SMB)

The newest SMB Version 1.5 provided by Microsoft for CE 5.0/ CE 6.0/ EC 7.0 is vulnerable against WannaCry.

Due to the fact Windows CE or EC can't execute standard windows x86 applications, the common known WannaCry wouldn't work.

Nevertheless the attack can evolve or could already have evolved and compiled for Windows EC/ CE ARM.

XV100/XC152/ Airmonitor/XV400/ XVS-400/XVH-400/ MK2/MC2/ MA2-450-20CAN

These devices run on Windows CE 5.0 and have SMB as standard deactivated.

Only if SMB is activated and the attacker has a compiled ARM Windows CE variant of WannaCry, the device is exposed to a potential WannaCry Ransomware attack.

So the overall risk regarding WannaCry is low

XV300

This device runs on Windows EC 7.0 and has SMB as standard deactivated.

Only if SMB is activated and the attacker has a compiled ARM Windows EC variant of WannaCry, the device is exposed to a potential WannaCry Ransomware attack.

So the overall risk regarding WannaCry is low

XC 200 Family

This device does not contain the SMB protocol.

So there is no risk regarding WannaCry.

Recommendation

Deactivate and/ or keep SMB deactivated as described in manual.

In general we recommend protecting devices written in Eaton's white paper for [Cybersecurity considerations for electrical distribution systems](#)

Best practices

- Always install newest Firmware update from EATON and only from EATON
- Protect access to physical Ports and cabinet
- Deactivate unused ports/ services
- Change passwords regularly
- Always use least privilege



Powering Business Worldwide

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

© 2017 Eaton
All Rights Reserved
Printed in XXX
Publication No. BRXXXXXXXE / XXX
April 2018

Follow us on social media to get the latest product and support information.



Eaton is a registered trademark.

All other trademarks are property of their respective owners.