

Date:	05.04.2018
Subject:	WannaCry Ransomware Analysis
Severity rating:	High
Product:	XP device family

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 \$300 or \$600 ransom in Bitcoin 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)

XP 503

XP 503 runs on Windows Embedded Standard 7 as operating System. It is based on Windows 7, which exposes XP 503 to a potential WannaCry Ransomware attack, in the following and older versions of XP 503:

Visual Designer

- SW Rel. 2.00.00

Galileo

- SW Rel. 01.03.00

In order to prevent an infection of WannaCry Ransomware in your network, apply the latest security patch

- Security Update KB4019264

which can be found in the Eaton Downloadcenter

<http://applications.eaton.eu/sdlc/?CX=94&LX=11>

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

Best practices

- Always install newest 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. BRXXXXXXXXXE / XXX
July 2017

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.