Cyber Security Notification - WannaCry Ransomware

Update Date: *none (original document)*

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Affected Products

No ABB products are directly affected, all Windows-based systems including ABB products running on Windows are potentially affected

Summary

On May 12th, 2017 the ransomware known as WannaCry or WannaCrypt was detected.

As most other ransomware as well, WannaCry uses social engineering via e-mail as its primary infection vector. However, once a system is compromised WannaCry can spread like a worm without user interaction by leveraging vulnerabilities in the Server Message Block (SMB) protocol. The SMB provides shared access to files, printers, and miscellaneous communications between nodes on a network.

The malware does not target any ABB products specifically, but, as any Windows-based system, also ABB systems may be susceptible to WannaCry. The vulnerability is not in the ABB software.

A Microsoft Security Update has been published in March 2017, which fixes the exploited SMB vulnerability in supported versions of Microsoft Windows. On May 13th, 2017 updates for Windows XP and Windows 2003 were released. There is generic advice with more information about the ransomware and how to mitigate it, e.g. from Microsoft or US-CERT and ABB recommends to consult the respective websites for obtaining such information.

ABB recommends several countermeasures to be part of any cyber security management program for industrial control systems and generally systems using ABB software. These countermeasures include

- Patch management
- Malware protection management
- Network security, especially the use of demilitarized zones with restrictive firewall rules regarding file sharing
- System hardening
- Backup and recovery management
- User awareness training

ABB also has service offerings which help customers to implement these recommended countermeasures and to maintain a high security level in systems running ABB software across the lifetime of the system.

This document describes specific actions that ABB recommends customers to take immediately to mitigate the threat of WannaCry, especially if they have not yet been following the general ABB recommendations or subscribed to the ABB cyber security services.

Recommended immediate corrective actions

ABB recommends that customers apply the following countermeasures immediately.

- Block or restrict Windows File Sharing via the SMB protocol as much as possible

  This will help to prevent spreading of the WannaCry malware from individual compromised computers. For specific guidance please see additional communication for specific ABB solutions and contact your local ABB service organization.

- Check options to install the Microsoft security update MS17-010

  This will help to prevent the infection of computers with the WannaCry malware both via malicious e-mails as well as via Windows File Sharing.

  Where applicable, refer to the 3rd party security updates qualification process. Results will be communicated through the usual documents.

- Update the malware protection / antivirus solution on your system

This will help to detect and block several variants of the WannaCry malware for which McAfee and Symantec have provided signatures in the meantime.

- Take a backup of your system

  Take an additional backup of the system and store it in a separate location (i.e. one that is not network-accessible from the system). This will enable you to restore operations should you become a victim of WannaCry despite all the other measures above.

Vulnerability Details

See https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.