Cyber Security Notification - NotPetya Ransomware

Update Date: 2017-07-06

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 June 27th, 2017 the ransomware known as NotPetya was detected.

As most other ransomware as well, NotPetya uses social engineering via e-mail as its primary infection vector. However, once a system is compromised NotPetya can spread like a worm without user interaction by leveraging vulnerabilities in the Server Message Block (SMB) protocol. The SMB may provide shared access to files, printers, and miscellaneous communications between nodes on a network. Reportedly, this is the same vulnerability that was already exploited by the WannaCry ransomware in May 2017. In addition, NotPetya reportedly can obtain credentials from the infected computer and use these credentials to infect adjacent computers it can reach on the network.

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

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 remote sessions for file sharing or command execution
- 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 NotPetya, 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 remote sessions for file sharing or command execution
- Check options to install the Microsoft security update MS17-010
- Update the malware protection / antivirus solution on your system
- Take a backup of your system

Product related corrective action or resolution

The following product specific guidance is available:

- SECURITY Notification – NotPetya Ransomware, impact on System 800xA,

  http://search.abb.com/library/Download.aspx?DocumentID=3BSE089835&LanguageCode=en&DocumentPartId=&Action=Launch

  This document and more relevant information is available for registered users on myABB/My Control System.

Vulnerability Details

See https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

Support

For additional information and support please contact your local ABB service organization. For contact information, see http://new.abb.com/contact-centers.

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