CrashOverride/Industroyer Malware

Update Date: 2017-06-30

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.

Summary

Recent investigations by cyber security experts have revealed a malware called CrashOverride or Industroyer that can exploit power domain specific communication protocols such as IEC 60870-5 101/104, IEC 61850 as well as OPC interfaces. The malware is characterized as a threat focusing on power systems and reportedly was involved in the blackout in Ukraine in December 2016.Investigations show that the malware has specific knowledge about ABB products.

We are in contact with concerned security companies and applicable authorities to gather and analyze additional information to provide more detailed guidance to our customers.

This notification aims to inform about the case and about important related information in connection with ABB products. Information related to specific ABB products is set forth below in this notification.

Product related Corrective Action or Resolution

The following product specific guidance is available:

- MicroSCADA Pro SYS600 and CRASHOVERRIDE, http://search.abb.com/library/Download.aspx?DocumentID=9AKK107045A0857&LanguageCode=en&DocumentPartId=&Action=Launch
- PROTECTION AND CONTROL MANAGER - PCM600 AND CRASHOVERRIDE, http://search.abb.com/library/Download.aspx?DocumentID=1MRS228757&LanguageCode=en&DocumentPartId=&Action=Launch
- SECURITY Notification - CRASHOVERRIDE/Industroyer malware, impact on System 800xA, http://search.abb.com/library/Download.aspx?DocumentID=3BSE089765&LanguageCode=en&DocumentPartId=&Action=Launch

General Risk Mitigation Measures

In addition to any specific recommendations mentioned above, ABB recommends several countermeasures to be part of all cyber security management program for industrial control systems and generally systems using ABB products and software. These countermeasures include:

- Patch management
- Malware protection management
- Cyber security assessment
- Perimeter protection
- 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 that 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.

Support

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

In case your system has been delivered by any of ABB's partners, additional information and support can also be provided by the partner.

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