Cyber Security Notification

Date

June 13, 2017

MicroSCADA Pro SYS600 and CRASHOVERRIDE/INDUSTROYER

Update Date: June 19th 2017

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.

ABB Oy
Power Grids,
Grid Automation
P.O. Box 614
FI-65101 Vaasa
FINLAND

Visiting Address
Strömberg Park,
Virtaviiva 9 A, 2nd floor
FI-65100 Vaasa
FINLAND

Phone: +358 102211
Fax: +358 1022 47133
e-mail:
first name.last name
@fi.abb.com

Business identity code:
0763403-0
Domicile: Helsinki

www.abb.com
www.abb.fi

Background

Public reports of preliminary investigations by cyber security experts have revealed a malware called CrashOverride or Industroyer. The reports indicate that the malware 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 also involved in the blackout in Ukraine in December 2016.
Such public reports also indicate that the malware is designed as a framework that can potentially be extended to other industry standard protocols such as DNP which generally makes it a threat for automation systems in the power industry.
This notification aims to inform about the case and about important related information in connection with MicroSCADA Pro.

Affected products

MicroSCADA Pro.

According to such public reports the malware also has specific knowledge about our ABB MicroSCADA Pro system. Up to now, no vulnerabilities have been identified in MicroSCADA Pro that would have allowed the malware to infect the system.

Continued activities

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

Risk mitigation

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 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.

This document describes specific actions that ABB recommends customers to take immediately to reduce their risk with possible malware, especially if they have not yet been following the general ABB recommendations or subscribed to the ABB cyber security services.

Upgrade:

We recommend to stay current on the latest software; for MicroSCADA Pro this is SYS600 9.4, which includes enhanced cyber security.

Enhanced cyber security protection of the system against malicious attack is improved in various ways, while new tools and functions make the configuration tasks as easy as possible. Among the new features are:

- An updated tool for deploying Windows security with preconfigured settings for various computer types such as servers and workstations
- Encrypted communication between SYS600 nodes
- Central User Account management with SDM600
- Role based access control
- Secure logging of user session events with reporting to SDM600 or 3rd party security systems
- Access control and authentication on the OPC Server interface

Support

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

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 http://www.abb.com/cybersecurity.