SECURITY Notification - CRASHOVERRIDE/Industroyer malware, impact on System 800xA

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.

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 reports however also indicate that the malware is designed as a framework that can potentially be extended to other industry standard protocols. This makes it a general threat for automation systems in the power industry.

Scope of this document

This document is a complement to the document Cyber Security Notification CrashOverride/Industroyer Malware (9AKK107045A1003) which is available under www.abb.com/cybersecurity → Alerts and notifications.
This document provides additional information specific for System 800xA.

Affected Products

System 800xA uses OPC internally. The system option “800xA for IEC 61850” uses IEC 61850. The malware reportedly uses OPC and IEC 61850, but up to now, no vulnerabilities have been identified in System 800xA that would have allowed the malware to infect the system.

Recommended immediate corrective actions for System 800xA

All the generic recommendations in Cyber Security Notification CrashOverride/Industroyer Malware (9AKK107045A1003) apply also for System 800xA.

Additional recommendations:

- Install the latest verified virus definition files for McAfee or Symantec.
- Consider applying 800xA Whitelisting SE46.
- Install the latest verified security updates from Microsoft.
- Upgrade to the latest version of System 800xA to benefit from the most recent security improvements from ABB

The verification status of virus definition files from McAfee and Symantec is described in the document *System 800xA Daily Verification of McAfee & Symantec updates (9ARD170703-011)*.

The verification status of the Microsoft security updates is described in the document *Microsoft Security Updates Validation Status (3BSE041902)*.

Security updates from Microsoft and virus definition files for McAfee’s and Symantec’s antivirus which have been verified by ABB can be installed using ABB’s *Security Update Service*.

ABB verified security updates from Microsoft can also be installed using *The System 800xA Qualified Security Updates for 800xA* 9ARD183777-017 (for System 800xA Version 5.1) and 9ARD183777-020 (for System 800xA Version 6.0).

ABB recommends its control system users to have a valid Automation Sentinel agreement for each of their installed control systems. Automation Sentinel, ABB’s control system life cycle management and support program, enables ABB control system users to receive verified Microsoft security updates and anti-virus verification reports.

ABB also recommends all users of System 800xA to request access to myABB/My Control System via their local ABB contact or our webpage myABB/My Control System for access to product documents (e.g. user manuals, data sheets, product updates, alerts, safety reports) and software downloads pre-filtered for their installed control system.
Basic access to My Control System is available for all ABB control system users.

For premium access to the myABB/My Control System web portal including access to verification results and downloadable qualified third party security updates, a valid Automation Sentinel agreement, is required for each control system.

The above referenced documents *9ARD170703-011*, *3BSE041902*, *9ARD183777-017 and 9ARD183777-020* are available on MyABB/My Control System for customers with a valid Automation Sentinel life cycle agreement.

Support

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

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