Cyber Security Notification - TRITON/TRISIS malware

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

The TRITON or TRISIS malware is targeting Industrial Control Systems (ICS), specifically one non-ABB brand of Safety Instrumented Systems. It uses proprietary and product specific communication protocols. Up until now, no vulnerabilities have been identified in ABB products that the TRITON or TRISIS malware can use to attack a system and no ABB products are affected directly by TRITON or TRISIS. However, conceptually a similar attack can be leveraged against any safety system with a sufficiently similar design concept.

Summary

On December 14th, 2017 an incident which reportedly has happened at a critical infrastructure operator was reported publicly, referred to as TRITON or otherwise TRISIS. A targeted malware compromised an engineering station of a safety instrumented system (SIS) and further manipulated function code and control logic on a safety controller of the SIS. The malware disguised as a legitimate application of the SIS and utilized the proprietary communication protocol of the specific product used at the target environment. While currently we have no indication that a similar malware exists which is targeting other safety products, conceptually the attack scheme can also be used against any sufficiently similar safety system, incl. ABB systems.

Recommended immediate actions

ABB recommends to strictly follow the guidelines as published in the relevant documentation of the respective product(s).

Additional recommendations:

- Networks used for Industrial Control Systems (ICS) should always be segregated from enterprise and/or public networks.
- Install vendor validated patches to the engineering system Operating System.
- Install the updated virus definition files for the recommended / supported malware protection solution.

Product related recommended immediate actions

The following product specific guidance is available:

- Security Notification - TRITON/TRISIS malware, impact on System 800xA High Integrity, http://search.abb.com/library/Download.aspx?DocumentID=3BSE090967&LanguageCode=en&DocumentPartId=&Action=Launch

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

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.