Cyber Security Notification - Meltdown & Spectre

Update Date: 2018-02-16

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

At the time of this publication, we are still investigating the affected ABB products. However, all ABB products that run on affected processors are potentially affected.

Summary

On January 3rd, 2018 two vulnerabilities, Meltdown (CVE-2017-5754) and Spectre (CVE-2017-5753 and CVE-2017-5715), affecting processors were made public.

Meltdown and Spectre are two vulnerabilities that affect processors and permit attackers to gain unauthorized access to a computer's memory. Subsequently, a successful exploit could allow attackers to gain access to any sensitive data, including passwords or cryptographic keys. Exploiting these vulnerabilities requires external code to be executed on the target.

The vulnerabilities do not target any ABB products specifically, but potentially affect products that use affected processors in general.

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 should always be segregated from enterprise and/or public networks.
- Install validated patches according to ABB's patch qualification and further product specific recommendations.
- Install the updated virus definition files for the recommended / supported malware protection solution.
- Prevent or reduce the execution of external code on Industrial Control Systems.

Product related recommended immediate actions

The following product specific notifications are available:

- SECURITY Notification - Meltdown & Spectre, impact on System 800xA, http://search.abb.com/library/Download.aspx?DocumentID=3BSE091052&LanguageCode=en&DocumentPartId=&Action=Launch.
  This document and more relevant information is available for registered users on myABB/My Control System.
- Cyber Security Notification - Meltdown & Spectre, impact on Symphony Plus, http://search.abb.com/library/Download.aspx?DocumentID=8VZZ000522&LanguageCode=en&DocumentPartId=&Action=Launch
- Cyber Security Notification - Meltdown & Spectre, impact on MicroSCADA Pro products, http://search.abb.com/library/Download.aspx?DocumentID=1MRS257754&LanguageCode=en&DocumentPartId=&Action=Launch
- SECURITY Notification - Meltdown & Spectre, impact on Freelance, http://search.abb.com/library/Download.aspx?DocumentID=2PAA117368D0002&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 https://new.abb.com/contact-centers.

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