Cyber Security Notification - Meltdown & Spectre, impact on Symphony Plus

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

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

These 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.

Scope of this document

This document is a complement to the document Cyber Security Notification - Meltdown & Spectre (9AKK107045A8219) which is available under www.abb.com/cybersecurity → Alerts and notifications.

This document provides additional information specific for Symphony Plus Products.

Affected Products

The vulnerabilities announced are not regarding ABB products specifically, but potentially impact ABB products that use affected processors in general, therefore ABB is currently evaluating and testing available patches for all potentially affected products.

Recommended immediate corrective actions for Symphony Plus systems

ABB has completed initial testing of Symphony Plus Systems to determine potential impact from the security updates that various vendors have released to address the Meltdown and Spectre vulnerabilities. Additional testing and updated information may be possible as the situation may warrant.

There are some unique conditions associated with the proposed updates which go beyond the normal installation of security updates. To address these vulnerabilities a number of actions will be required to include:

- Installation of Microsoft issued security updates for the various Operating System versions to address these processor vulnerabilities. Unlike traditional security updates, these require a registry keys/settings to allow them to install and to take effect.
- While Microsoft has released patches to address the vulnerability, in most cases microcode/BIOS updates may be also recommended by the computer hardware manufacturers to further enhance protection.
- Anti-Virus applications will need updates due to potential negative impacts from this security patch. Approved AV vendors have included the necessary registry key to allow the installation of the Microsoft Patch.

Detailed instructions on the proper methods and sequence to update systems are being provided to assist users. Below is a list of relevant documents which should be reviewed prior to implementing the necessary updates:

- Cyber Security Notification Meltdown Spectre on Symphony Plus (8VZZ000522)
- Security Updates Validation Status for Symphony Plus (2VAA001442)
- Security Updates Validation Status for PGP (9AJG000036)
- Security Updates Validation Status for Procontrol P14 (2VAA009056)
- Security Updates Validation Status for 800xA for PG (9AJG000035)
- Technical Description Updating Computers for Spectre & Meltdown (3BSE091125)

Additional information for Symphony Plus systems

As with all security patches which are tested, ABB attempts to evaluate whether the updates introduce any functional issues which impact Symphony Plus systems. None of the updates identified in the above documents were found to inhibit the normal operation of the applications listed.

Additionally due to concerns that these patches may degrade CPU speed, some performance testing was also conducted in this monthly cycle. Initial results do not show significant impact however the variety of system configurations which are available internally does not cover the diversity present in the various systems installed world-wide. As mentioned above, OEMs are releasing microcode/BIOS updates which may impact overall performance as well. Stable versions of microcode were not available at the time of this testing therefore the evaluation does not include such. End users are advised to implement these updates with care and evaluate the impact on performance within their own environments.

Please note that, based on our current understanding of the Meltdown and Spectre vulnerabilities, the embedded devices in various Power Generation product families do not utilize the vulnerable functions (i.e. speculative execution and memory access protection) in a way that they can be used to disclose confidential information as described in the publicly available vulnerability reports. The devices include controllers, I/O and communication modules of the following:

- Symphony Plus SD Series
- Symphony Plus HR Series (Harmony Rack)
- Symphony Plus MR Series (Melody Rack)
- Procontrol P14
- Procontrol P13
- DCI System Six
- Symphony Harmony
- Symphony Melody
- INFI 90

Vulnerability Details

See https://support.microsoft.com/en-us/help/4073757/protect-your-windows-devices-against-spectre-meltdown

Subscribe to ABB Alerts and Notifications LINK and ensure current enrollment in ABB Power Generation Care or ABB Water Care to get further updates.

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.

Revision

Rev.ind.	Page (P) Chapt. (C)	Description	Date Dept.
A	All	New document	2018-01-15 IAPG
B		Updated description	2018-01-18 IAPG
C		Added information on embedded devices	2018-01-22 IAPG
D	multiple	“Initial Indications” are replaced with “Corrective Actions”	2018-02-02 IAPG