Cyber Security Notification
Meltdown&Spectre impact on MicroSCADA Pro products

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.
Copyright © 2018 ABB. All rights reserved.

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 products:
- MicroSCADA Pro SYS600/SYS600C
- MicroSCADA Pro SYS600 Historian
- MicroSCADA Pro DMS600
Affected Products
The vulnerabilities do not target any ABB products specifically, but potentially impact 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 MicroSCADA Pro products
ABB has completed initial testing of MicroSCADA Pro products 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:

- Antivirus software will need updates due to not being compliant with Microsoft security update. Approved antivirus software vendors have included the necessary registry key to allow the installation of the Microsoft security update.
- Installation of Microsoft 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 updates to address the vulnerability, in most cases microcode/BIOS updates may also be recommended by the computer hardware manufacturers to further enhance protection.

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:

1. Cyber Security Notification - Meltdown&Spectre (9AKK107045A8219) (ABB’s generic recommendations related to Meltdown&Spectre)
2. Cyber Security Notification - Meltdown&Spectre impact on MicroSCADA Pro products (1MRS257754) (this document)
3. Technical description for updating Windows computers (1MRS257762) and Patch Compatibility Reports for SYS600 and DMS600 are available on MicroSCADA Pro Portal for system integrators and service.

Additional information for MicroSCADA Pro products
As with all security updates, which are tested, ABB attempts to evaluate whether these introduce any functional issues which impact the product. None of the updates identified in the above documents were found to inhibit the normal operation of the system.

Additionally due to concerns that these updates may degrade CPU speed, some performance testing was also conducted in this monthly cycle.

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. Users are advised to implement these updates with care and evaluate the impact on performance within their own environments.

**SYS600 and DMS600**: Initial results do not show any significant impact, however the variety of system configurations, which are available internally does not cover the diversity present in the various systems installed worldwide.

**SYS600 Historian**: Performance testing is still ongoing. Therefore, ABB refrains to make a recommendation whether to install the updates at this point in time.

**SYS600C**: Above mentioned results for SYS600 and DMS600 apply also for SYS600C. MicroSCADA Pro SYS600 Security Patch Compatibility Report will be updated once microcode/BIOS update is available and verified.

**Vulnerability Details**


**Support**

For additional information and support please contact your local ABB service organization. For contact information, see [www.abb.com](http://www.abb.com) and [www.abb.com/microscadapro](http://www.abb.com/microscadapro).

Information about ABB’s cyber security program and capabilities can be found at [www.abb.com/cybersecurity](http://www.abb.com/cybersecurity).
Revision

<table>
<thead>
<tr>
<th>Rev. ind.</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>New document</td>
<td>2018-01-25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PGGA/GAP</td>
</tr>
<tr>
<td>B</td>
<td>Updated after initial tests</td>
<td>2018-02-23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PGGA/GAP</td>
</tr>
</tbody>
</table>