9AKK107045A8431 SECURITY ANNOUNCEMENT

ABB Ability™ Operations Data Management zenon Windows 10 update causes driver communication problems

Due to major security leaks in Intel and AMD processors, Microsoft and other software / hardware vendors released new updates at the beginning of the year 2018

ABB has recognized a problem after applying the Windows Updates KB4056892 and KB4056891.

After applying these updates values from the zenon drivers are no longer delivered into the zenon Runtime system. The necessary processes are not affected, they keep on running and can still be seen in the task manager of the OS. .

ABB and its partners are currently working on analyzing the source of the problem with high priority. We have generated a ticket at Microsoft Tech Support in order to coordinate the activities. As it seems at the moment the problem cannot be solved by ABB alone, we are depending on the OS Updates from Microsoft.

Products affected
All zenon Runtime systems of generation 7.xx and their PLC drivers are affected by this problem.

Versions affected
All zenon versions of generation 7.xx seem to be affected. At the moment we have no reports of older systems that are showing this error scenario.

All Windows versions of generation 7, 8 and 10 seem to be affected.

Vulnerability details
Original Vulnerability Details from Intel which led to the OS Updates: On January 3rd, a team of security researchers disclosed several software analysis methods that, when used for malicious purposes, have the potential to improperly gather sensitive data from many types of computing devices with many different vendors' processors and operating systems.

These exploits are based on side-channel analysis. A side-channel is some observable aspect of a computer system's physical operation, such as timing, power consumption or even sound. The statistical analysis of these behaviors can in some cases be used to potentially expose sensitive data on computer systems that are operating as designed. These exploits do not have the potential to corrupt, modify or delete data.

Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

CVSS v3 base score and vector:
A CVSS base score of 8.2 has been calculated for this vulnerability. The corresponding CVSS v3 vector:

AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N

For Details check:

https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

Detection:
Real-time values are no longer delivered into the zenon driver. This can be recognized by:

- Missing values on a process screen

- Gaps in the zenon Historian data recording

- Missing alarms end events

- Etc.

Other components affected:

Beside the communication between the zenon driver and the zenon Runtime no other components are affected.

Restore normal operation:
A restoring to normal operation without de installing the above mentioned Windows Updates is not possible.

Mitigations
The only mitigation strategy at the moment is a roll-back of the Microsoft Windows Updates KB4056892 and KB4056891.

General recommendations
ABB and it's partners are applying continuous Windows patch testing in the context of the zenon Product Family to recognize problems at an very early stage. Beside this activities ABB generally recommends to test OS Updates before applying these to any productive system. Windows OS Patches should always be centrally managed and deployed company wide.

Acknowledgements
ABB wishes to thank the OEM's & Partners for reporting this issue and our consulting & development team for analyzing the issue and the ongoing efforts.

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.

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.