9AKK107045A8623 TECHNICAL ANNOUNCEMENT 18-01

# ABB Ability™ Operations Data Management zenon
# Windows updates cause data communication problems with zenon

2018-02-26

This announcement CLOSES issues reported in 9AKK107045A8623 TECHNICAL ANNOUNCEMENT 18-01

### Introduction

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

An issue with these updates has led to problems with zenon. The effect is a known issue in several Windows updates. The full list of affected products and operating systems is listed here: https://portal.msrc.microsoft.com/en-US/securityguidance/advisory/ADV180002.

After applying specific versions of the January 2018 updates, various communication issues may occur (more details can be found in the “detection” section of this document).

After a detailed analysis, we have verified verify that the issues recognized are based on the January 3rd security updates for various Microsoft Windows versions.

Microsoft has been working on a resolution of the known issue and is providing updated versions of the January 3rd security updates (regarding the following updates: 4056893, 4056888, 4056890, 4056891, 4056892, 4056898. This information was published on January 3rd by Microsoft).

### Products affected

Issues have been recognized within the following zenon product components:

- zenon Runtime and its drivers
- zenon remote transport
- zenon network

### Versions affected

The following supported zenon versions are showing the detected symptoms on systems where these issues occurred:

- zenon 8.00 (Beta)
- zenon 7.60
- zenon 7.50
- zenon 7.20

Older (no longer maintained zenon versions) may also be affected.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.

The issues have been documented under the following references:

- CVE-2017-5715

- CVE-2017-5753

- CVE-2017-5754

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, please check:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA00088&languageid=en-fr

### Detection

Some of the symptoms that have been detected after applying the above mentioned Microsoft security updates are:

- Error message on starting the zenon driver; drivers not running correctly
- Missing values on a process screen
- Gaps in the zenon Historian data recording
- Missing alarms and events
- No data availability and connectivity issues on zenon network clients
- Impacts on the remote transport

Other components affected:

Beside the above-mentioned issues, no other components are reported to be affected at current state.

### Restore normal operation

A recovery to normal operation can be achieved by uninstalling the above-mentioned Windows updates or by installing an updated version of the windows updates that resolve the issues.

### Mitigation

Mitigation is possible by preventing the installation of the Microsoft Windows updates containing the known issues and ensure that only the updated Microsoft Windows updates are possible to install.

Since the release of the original Windows Updates for the January 3rd security update with the known issue, Microsoft has released updated Windows Patches which address the original vulnerabilities but do not have a negative impact on the operation of the zenon components.

NOTE: the windows updates listed below may not all be automatically distributed via Windows Update / WSUS yet. In such case, manually downloading and installing the corresponding update, resolves the issue.

ABB and its suppliers have monitored and tested the following Microsoft Patches as a solution for the above-mentioned issues:

- KB4057401 resolves KB4056895 and KB4056898 - Windows 8.1 and Windows Server 2012 R2 Standard

- KB4057401 resolves KB4056898 - Windows 8.1. for x64-based Systems
- KB4057144 resolves KB4056891 - Windows 10 Version 1703 for x64-based Systems
- KB4075199 resolves KB4056893 - Windows 10 Version Enterprise
- KB4075200 resolves KB4056888 - Windows 10 Version 1511
- KB4073291 resolves KB4056892 - Windows 10 Version 1709
- KB4057402 resolves KB4056896 - Windows Server 2012 Standard
- KB4057142 resolves KB4056890 - Windows Server 2016 and Windows 10 1607

### General recommendations

ABB and its suppliers are applying continuous Windows patch testing in the context of the ABB zenon Product Family to recognize problems at a very early stage. Beside these activities, ABB generally recommends to test any OS updates before applying these to productive systems. Windows OS patches should always be centrally managed and deployed company-wide.

Other security strategies that should be in place in order to avoid the original security leak are documented in the zenon Security guidelines delivered with every zenon installation and can be requested at your local support team (e.g. Application Whitelisting).

### Acknowledgements

ABB thanks all zenon users who reported on this issue.

### 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.

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.

### Version information

| Date | Comment |
|---|---|
| 2018-01-16 | Initial Information |
| 2018-02-26 | Issues resolved and closed |