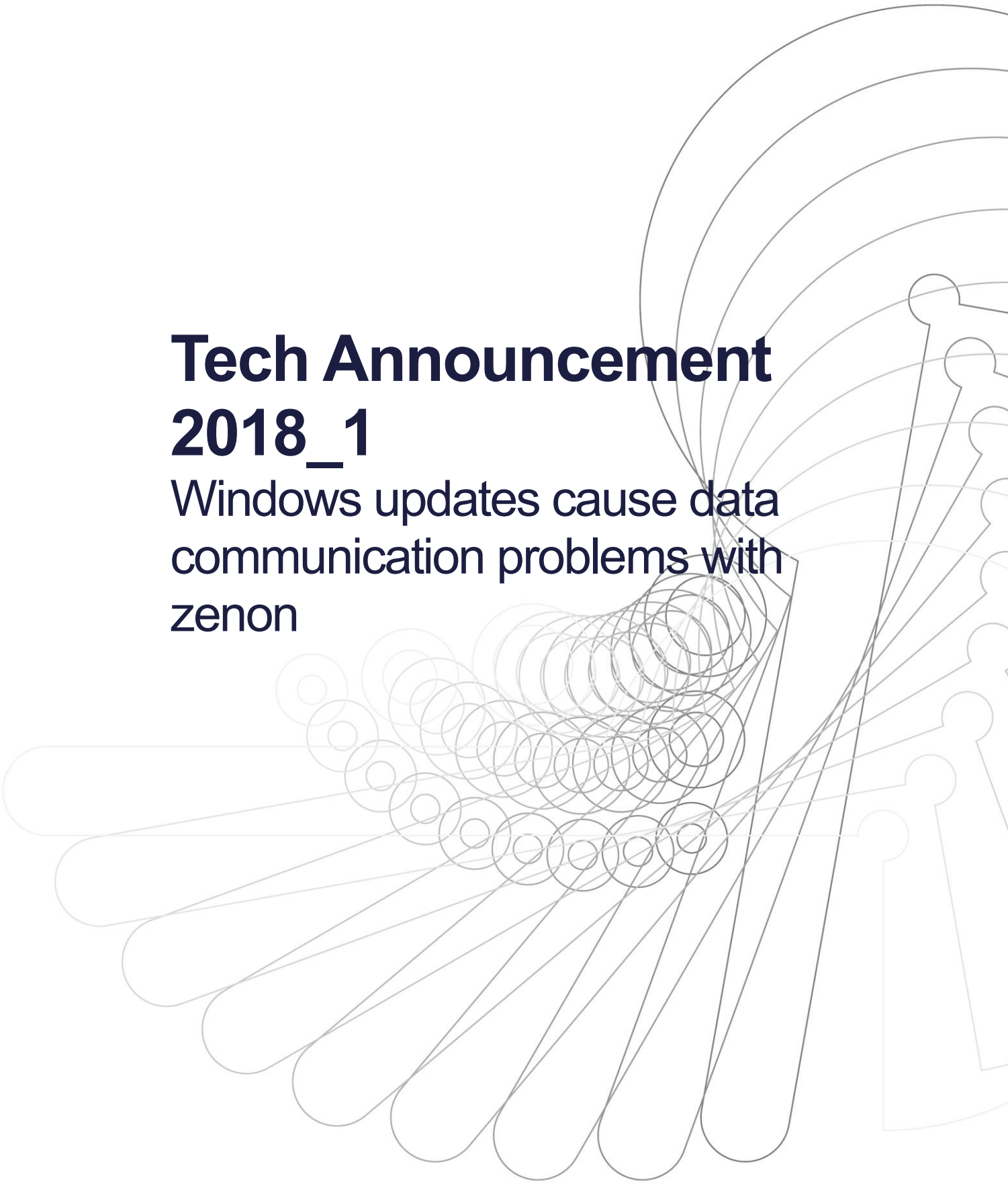
Tech Announcement 2018_1

Windows updates cause data communication problems with zenon



zenon®

History

Date	Comment
09.01.2018	Document version 1
16.01.2018	Document version 2

Content

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 in these updates leads to problems with zenon. The effect is a known issue in several Windows updates. The full list of affected products and operation systems are listed here: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002.

After applying one or several of these updates, various communication issues may occur (more details can be found in the “detection” section of this document).

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

Microsoft is working on a resolution in an upcoming release (regarding the following updates: 4056893, 4056888, 4056890, 4056891, 4056892, 4056898). This information was published on January 3rd by Microsoft.

COPA-DATA has generated a ticket at Microsoft Tech Support in order to coordinate activities and is urging on the case with high priority.

Microsoft is working on a resolution and we are waiting for the Windows updates that will fix these issues. Any new information will be communicated as soon as possible.

Products affected

Issues have been recognized within the following zenon product components:

- zenon Runtime and its drivers

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
- zenon 7.11

Older (no longer maintained zenon versions) might also be affected.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

Thi 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-SA-00088&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 without uninstalling the above mentioned Windows updates is not possible at the moment.

Mitigation

At the moment, the only mitigation strategy is a roll-back or deinstallation of the Microsoft Windows updates mentioned above.

General recommendations

COPA-DATA is applying continuous Windows patch testing in the context of the zenon Product Family to recognize problems at a very early stage. Beside these activities, COPA-DATA 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

COPA-DATA thanks all OEMs and Partners who reported on this issue.