Overview

This security bulletin follows alerts related to newly discovered CPU vulnerabilities dubbed Meltdown and Spectre. These vulnerabilities are being fixed by series of operating system updates and CPU micro-code updates.

ARC Informatique recommends users of its products to actively watch for software and hardware updates addressing Meltdown and Spectre. It is advised to test them prior to deployment on production system. Such tests should cover effectiveness**,** performances and regressions.

This article summarizes the timeline and addresses concerns related to the Microsoft Windows updates designed to mitigate these vulnerabilities.

Early January - A first series of Windows Updates

A first series of Microsoft Windows Updates designed to mitigate the Meltdown & Spectre vulnerabilities has been rolled out early in January. As described on the Microsoft web site, they come with a known issue affecting applications based on the COM technology, including PcVue, FrontVue and some partner products.

Microsoft Update references - First series:

- KB4056888 - Windows 10 Version 1511
- KB4056890 - Windows 10 Version 1607 and Windows Server 2016
- KB4056891 - Windows 10 Version 1703
- KB4056892 - Windows 10 Version 1709
- KB4056893 - Windows 10 RTM (initial version released July 2015)
- KB4056895 - Windows 8.1 and Windows Server 2012 R2
- KB4056896 - Windows Server 2012
- KB4056898 - Windows 8.1 and Windows Server 2012 R2
- KB4056899 - Windows Server 2012

Note that Windows 7 SP1 and Windows Server 2008 R2 SP1 do not seem to be affected by the issue, despite the following updates roll-up:

- KB4056894 - Windows 7 SP1 and Windows Server 2008 R2 SP1
- KB4056897 - Windows 7 SP1 and Windows Server 2008 R2 SP1

(These lists may be incomplete)

Symptoms of the CoInitializeSecurity issue

The *CoInitializeSecurity* issue prevents affected products from working as expected in some of the most usual circumstances.
Typical side effects of this issue are:

- PcVue starts, but the Historical Data Server does not archive any data, in fact it cannot connect to the Sv32.exe process,
- Fatal error (AIExplorer.exe) when launching the Application Explorer or the Application Architect.

Other features may also be affected:

- Tools connecting to the PcVue configuration server interface may be affected including Smart Generators, Command line tool for XML Generic import...

The issue affects software components that include a COM client. Among them, OPC-DA clients as well as many inter-process interfaces.
As extracted from the Microsoft articles (known issues):
"When calling CoInitializeSecurity, the call may fail when passing RPC_C_AUTHN_LEVEL_NONE as the authentication level. The error returned on failure is STATUS_BAD_IMPERSONATION_LEVEL."

Solution

As a temporary workaround, and until the fix is available, the specific Windows Update has to be uninstalled from affected computers to ensure PcVue runs correctly and fulfill its duties for all features and functionality used in your project.

Important note:

The Microsoft wording says 'the call may fail'. **The issue is affecting some computers, but not all of them.** As a consequence, it is a must to test these Windows updates on your specific hardware and software prior to deploying them on production systems.

January 17th - A second series of Windows Updates

On January 17th, Microsoft started rolling out fixes delivered via Windows Update. They address the CoInitializeSecurity issue coming with the first series of updates.

- KB4057142 - Windows 10 Version 1607 and Windows Server 2016
- KB4057144 - Windows 10 Version 1703
- KB4057401 - Windows 8.1 and Windows Server 2012 R2
- KB4057402 - Windows Server 2012

Be aware that some of these updates are 'Optional', and depending on the Windows update configuration, they may not be installed automatically. More updates are expected in the coming days to cover Windows 10 Version 1511, Windows 10 Version 1709 and Windows 10 RTM.

How to protect your system

For more information about these vulnerabilities and how to protect your system, you can refer to the following Microsoft articles:

- The original advisory from Microsoft
- Guidance for desktop computers
- Guidance for servers
- Guidance for SQL Server

What is the impact on performances

According to various sources, mitigation of the Meltdown and Spectre may come with a performance impact ranging from almost no degradation to a significant overhead, depending on the exact CPU vendor/model/version and the types of workload. Because benchmarks are difficult to establish in such a situation, we invite users to assess the potential impact on performances in their own environment prior to deployment in production.

References

- Vulnerability Note VU#584653
- ICS-CERT alert: ICSA-ALERT-18-011-01B
- CVE-2017-5753
- CVE-2017-5715
- CVE-2017-5754
- The public ARC Informatique security alert page: www.pcvuesolutions.com
- The Knowledge Base article for more information: support.pcvuesolutions.com

Want to report a vulnerability or provide feedback – Please email us at secure@arcinfo.com

Document history

Revision	Action	Date
1.0	First publication	23/01/2018