Security Advisory Meltdown & Spectre

Meltdown and **Spectre** are two attack scenarios that exploit a security vulnerability in certain CPUs from different manufacturers (Intel, AMD, ARM). For this purpose, a special code (program) is inserted and executed on a device. This code can read out the data of a CPU function which retrieves the information that may be required later for all parallel running programs in advance. This CPU function is called Speculative Execution and has been used throughout the industry for years to speed up data processing on the CPU.

The vulnerabilities have already been discovered by the **Project Zero Team** of Google Inc. already in mid-2017. They also point to the two attack scenarios developed by a team of highly specialized security experts.

To remedy the CPU vulnerability, the manufacturers of operating systems (Linux, Windows, iOS, Android) rely on a technology called “kernel page-table isolation” (**KPTI**, formerly KAISER). At the present time, corresponding updates and patches are already generally available. If necessary, please observe the current information of the relevant manufacturers.

No Endangerment

Dallmeier camera and recording systems are equipped with a **Linux operating system** that is strongly adapted hardened with regard to system security. It does **not offer any possibility** to **import or execute an external program**. Irrespectively of the CPU used, there is therefore **no danger from** the published attack scenarios **Meltdown and Spectre**.

*Dallmeier **camera and recording systems** are equipped with a **Linux operating system** that is strongly adapted and hardened. They are **not endangered** by the currently published CPU security vulnerability.*

Endangerment

In general all **computer systems with Microsoft Windows operating systems** are at risk and thus also various Dallmeier products such as for example:

- Workstation Tower
- Workstation Rack-Mount 4RU
- Server Rack-Mount 1RU
- Discontinued products such as PView Station 7 or SeMSy® III Workstation Hardware

Dallmeier products with Windows operating systems are always delivered with the latest updates and security patches released at the time of production.

Procedure

Basically, the **Microsoft Windows operating system** should always be kept **up to date**. This can be done directly via the update function of the operating system. However, Microsoft also informs about the latest update on the following web page:

Refer to the information posted on the web page regarding limited compatibility of the update with certain versions of antivirus software.

https://support.microsoft.com/en-us/help/4056890/windows-10-update-kb4056890

Keep computer systems with Windows operating system up to date with the latest updates and security patches.

In addition to a current operating system, the **established measures and procedures of IT security** should always be observed.

- Perform regular backups of important data
- Use current virus anti-virus software
- Use current web browsers
- Avoid the execution of suspicious files
- Avoid running scripts or macros
- Raise employee awareness

Never start an executable file that does not seem to be 100 % trustworthy. Make your employees aware of this.

Windows XP

Computer systems with a **Microsoft Windows XP** operating system should be **disconnected** immediately from the **network and in particular from the Internet**.

The **Windows XP** operating system is hopelessly **obsolete** (End of Life). Microsoft does not offer **any updates or support** (End of Support) since 2014. For more information, visit the following Microsoft web site:

https://www.microsoft.com/en-us/windowsforbusiness/end-of-xp-support

The Dallmeier sales team or your sales partner will be pleased to advise you on migration to computer systems with a modern Microsoft Windows 10 operating system.