KYOCERA Document Solutions Europe B.V.
Bloemlaan 4
2132 NP Hoofddorp, The Netherlands
http://www.kyoceradocumentsolutions.eu/

SPECTRE & MELTDOWN CPU VULNERABILITY STATUS ON KYOCERA DEVICES

1.0 Summary

In January 2018, security researchers reported computer hardware vulnerabilities called "Meltdown" and "Spectre". Exploitation of these vulnerabilities could allow an attacker to obtain access to memory areas in computers which are normally inaccessible. As a consequence passwords, personal information, emails, financial data and other sensitive documents could be compromised.

These vulnerabilities have been registered as CVE-2017-5753, CVE-2017-5715 (Spectre) and CVE-2017-5754 (Meltdown). The CVSS* score is medium (5.6) and the exploitability score** is relatively low (1.1) due to restrictive attack conditions.

* Common Vulnerability Scoring System = a numerical score reflecting the severity of a vulnerability
** This score reflects the ease and technical means by which the vulnerability can be exploited

The majority of systems in the field using Intel, AMD and ARM processors is considered vulnerable, i.e. not only personal computers or servers but also smart phones, cloud systems or – among many other categories of equipment – printers and multifunction systems.

Performing exploits on Meltdown and Spectre requires the access to the operating system inside a device and the execution of malicious code within this system. The vulnerability is mainly concerning read access to memory, whereas manipulation of data and execution of malicious code can't be easily performed.

Detailed information on both vulnerabilities is available here: https://meltdownattack.com/

2.0 Risk to KYOCERA Devices

KYOCERA devices contain ARM CPUs as part of embedded systems in a "Closed Platform" concept, with none or very limited exposure to the outside of the device. This effectively prevents any unauthorised software to be executed.
Those devices that allow execution of software are protected by a digital signature concept controlled by KYOCERA. Any attempt to upload unauthorised components or modify installed software components will be detected and discarded.

Potential attacks through print jobs: Although print jobs typically contain PostScript, PCL or PJL commands to be executed by the printer to form a print job or respond to a status request, these commands are executed within a special interface within the controller with strictly limited read and write capabilities. It is therefore not possible to perform a Spectre or Meltdown based attack on KYOCERA printers and multifunction devices.

Due to the existing security concept, KYOCERA considers the risk to printer and multifunction devices very low.

3.0 Risks to the EFI Fiery System

Several KYOCERA multifunction devices can be (optionally) equipped with an EFI Fiery digital front end for an improved workflow, higher processing speed and standardised colour matching.

EFI Fiery devices are available as a Linux or Windows based version, both utilising CPUs which are considered vulnerable.

Official information on potential threats and countermeasures is provided on the following web page:

http://www.efi.com/ja-jp/support-and-downloads/kbarticle/article-details/?knowledgeArticleID=kA339000000HCDaCAO

KYOCERA devices are equipped with the Linux based Fiery device; according to above statement EFI is not aware of any impact to these devices due to the security concept inherent to the system.

4.0 Risks to KYOCERA Software Products

Among the software products offered by KYOCERA, only cloud based systems might have a risk to be affected by this vulnerability.

KYOCERA Fleet Services (KFS) are built on the Microsoft Azure cloud computing platform. Microsoft has already implemented all necessary countermeasures to address this threat, therefore KFS is not vulnerable to Spectre or Meltdown based attacks.

Official information is provided by Microsoft here:

https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/