Canon

February 16, 2018
Updated: March 16, 2018
Canon Inc.

Regarding the CPU vulnerabilities Meltdown and Spectre

Recently, CPU vulnerabilities known as Meltdown and Spectre were made public.

When malicious software is installed on products and executed, these vulnerabilities can enable access to data that would usually be inaccessible.

Regarding the impact of these vulnerabilities on Canon products, as of now, we believe that the products and services that may be affected are listed below:

- imagePRESS Server/ColorPASS/imagePASS: EFI has announced the status of their response on their public website.
  http://www.efi.com/support-and-downloads/kbarticle/article-details/?knowledgeArticleID=kA339000000HCDaCAO
- imagePRESS CR Server
- Canon Business Imaging Online MDS Cloud: OS Patch has been applied.
- Canon Business Imaging Online Forms and Print Services for Salesforce: OS Patch has been applied.

We have yet to confirm that users of these products have been affected as a result of these vulnerabilities. However, to protect against these vulnerabilities, we are taking countermeasures such as software patches in order to ensure users to continue using Canon products with peace of mind.

We are currently unaware of any other Canon products that are vulnerable to the disclosed attack methods of Meltdown and Spectre.

In the event that new attack methods relating to these vulnerabilities are disclosed that we determine could affect Canon products, we will update this information as necessary.

Contact Information

Should you have any questions about this notice, you may contact us directly.