XSS Fix FAQ

Is there any countermeasure available?

Yes, Kyocera has developed a countermeasure against the Vulnerability of the Command Center by releasing Firmware* updates for the effected machines (see the details within this XSS FAQ Bulletin).
Please contact your local dealer or Kyocera support to receive the latest Firmware for your device.

Recommended workaround

When it is necessary to access other web sites in case your device still operates with a Firmware Version without including the XXS Vulnerability fix.

When accessing our products (via the command center) and other web sites at the same time, it is possible for this vulnerability to exist when running the older Firmware* versions on some of our devices.

In such cases do not access other web sites at the same time while accessing our products via the command center before you have updated the firmware of the related Kyocera device.

* Below Firmware versions have included the Firmware Fix

FS-C2026MFP, FS-C2126MFP	- Version 09.16.0010 or higher [2KW_2F00009003]
FS-C2526MFP, FS-C2626MFP, TASKalfa 265ci	- Version 08.16.0010 or higher [2M8_2F00008005]
FS-C2026MFP+, FS-C2126MFP+	- Version 08.16.0010 or higher [2MA_2F00008005]
FS-3540MFP, FS-3640MFP	- Version 08.04.0010 or higher [2MC_2F00008005]
FS-C5150DN, FS-C5250DN	- Version 05.10.0010 or higher [2KV_3F00005003]
FS-C8020MFP, FS-C8025MFP	- Version 06.15.0010 or higher [2KZ_2F00.006.005]
FS-6030MFP, FS-6025MFP/FS-6025MFP/B	- Version 06.10.0030 or higher [2K3_2F00.006.005]