

# Bug Advisory

Title	Bug Advisory Concerning Software Reset Failure on ESP32-S3 After OTA Upgrade to Specific ESP-IDF Versions with Quad SPI Flash Access Frequency Increased to 120 MHz
Issue Date	2024/10/12
Advisory Number	AR2024-010
Serial Number	NA
Version	V1.0

## Determining If Your Application Is Affected

Confirm that the following conditions are met simultaneously:

1. You are using an ESP32-S3 series product.
2. The chip accesses quad SPI Flash in QIO, QOUT, or DIO mode.
3. The Flash access frequency of the application was increased from the original 80 MHz to 120 MHz via OTA.

If all of the conditions above are met, your application is affected.

## Issue Summary

If the device runs a second stage bootloader built without support for the HPM-DC feature, while the HPM-DC feature is enabled in the application via an OTA update, the application will fail to boot again after reset. This issue may happen silently when you increase Quad SPI Flash access frequency to 120 MHz via OTA on specific IDF versions.

See section "Affected ESP-IDF Versions" below to see under which conditions the application will enable the HPM-DC feature, and the second stage bootloader will have the support for it respectively.

Below is the description of the cause and the influence of the issue.

The function of running SPI Flash at 120 MHz is called High Performance Mode (HPM). Some SPI Flash requires a Dummy Cycle adjustment to enter HPM, and support for these SPI Flash is referred to as HPM-DC. This adjustment affects the access timing of QIO and DIO modes.

After adjusting the Dummy Cycle, if the chip resets without powering down the SPI Flash, the adjusted Dummy Cycle in SPI Flash will be retained. This prevents the ESP-IDF second stage bootloader (bootloader refers to the second stage bootloader hereinafter If not specified) from being loaded and starting properly, leading to continuous chip resets (invalid header) before running into applications. This issue can be temporarily resolved by powering down the Flash.

Since different SPI Flash chips need different configurations to run in QOUT mode, an ESP-IDF second stage bootloader using QOUT mode needs to be loaded by the first stage bootloader in DIO mode first. Therefore, applications using QOUT mode are also affected.

In ESP-IDF versions with the HPM-DC feature, the bootloaders were adjusted to be compatible with Dummy Cycle changes, ensuring proper loading and startup. However, if the device uses an earlier bootloader that does not support HPM-DC (See section “Affected ESP-IDF Versions” below) but upgrades to an application that enables HPM-DC via OTA, issues may arise.

Some ESP-IDF versions automatically enable HPM-DC when the SPI Flash access frequency is set to 120 MHz (`CONFIG_ESPTOOLPY_FLASHFREQ_120M`) in the application. If the bootloader doesn't support HPM-DC, the described issue will happen silently.

## Affected ESP-IDF Versions

Bootloader support for HPM-DC across different ESP-IDF versions:

- Versions before v4.4.4: No HPM-DC support.
- v4.4.4–v4.4.6, v5.0–v5.0.6, v5.1–v5.1.3:  
HPM-DC is supported when the `CONFIG_ESPTOOLPY_FLASHFREQ_120M` option is enabled.
- v4.4.7, v5.0.7, v5.1.4, v5.2 and above:

HPM-DC is supported when the CONFIG\_BOOTLOADER\_FLASH\_DC\_AWARE option is enabled. (See detailed information in the ESP-IDF Patched Versions table below).

The ESP-IDF versions that enable HPM-DC by default in the application when running at 120 MHz:

ESP-IDF Branch	Affected Commit IDs	Affected ESP-IDF Versions
release/v4.4	<a href="#">1411de5 - 5684098</a>	v4.4.4 – v4.4.6
release/v5.0	<a href="#">2989735 - 50fc2bf</a>	v5.0 – v5.0.6
release/v5.1	<a href="#">2989735 - db2a037</a>	v5.1 – v5.1.3
release/v5.2 and above	-	Not affected

When updating to these versions, please make sure the second stage bootloader supports the HPM-DC feature to avoid the issue.

## Mitigation

### ESP-IDF Patched Versions

ESP-IDF Branch	Fixed Commit IDs	Fixed ESP-IDF Versions
release/v4.4 (EOL)	<a href="#">5684098</a>	v4.4.7
release/v5.0	<a href="#">50fc2bf</a>	v5.0.7
release/v5.1	<a href="#">db2a037</a>	v5.1.4
release/v5.2 and above	<a href="#">d2d75ef</a>	v5.2

After the fixes, ESP-IDF functions as follows:

1. The HPM feature notifies more clearly about its dependency on specific SPI Flash devices. You need to ensure that the Flash chips used in your products support this feature, and that the ESP-IDF version supports these Flash chips.
2. The HPM-DC functionality in the second stage bootloader is no longer enabled by default. Users need to choose whether to enable it based on the specific situation:
  - a) For new projects, it is recommended to manually enable HPM-DC when using HPM.

- b) For applications compiled for OTA, users need to confirm their bootloader configuration before deciding whether to manually enable HPM-DC. For more details, see section “Affected ESP-IDF Versions” above.

When support for HPM-DC functionality in the bootloader is enabled, HPM-DC will be automatically enabled. Otherwise, this feature remains disabled.

For more details, see “SPI Flash API > Optional Features for Flash > High Performance Mode” section in [ESP-IDF Programming Guide](#).

## Recommendations for Application Developers

- If your application runs at 120MHz and the bootloader lacks HPM-DC support, avoid enabling HPM-DC via OTA.
- Ensure that flash chips requiring HPM-DC support are not used if the bootloader does not support HPM-DC.
- When enabling 120 MHz and HPM-DC features, carefully review the relevant documentation and configuration options.
- If issues arise during updates, refer to the “Affected ESP-IDF Versions” section above for guidance.

If you encounter any issue during the update, please record your current ESP-IDF version or commit ID and consult [Espressif](#).