Security Advisory

Title	Security Advisory for USB_OTG & USB_Serial_JTAG Download Functions of ESP32-S3 Series Products
Issue date	2022/06/01
Advisory Number	AR2022-004
Serial Number	NA
Version	V1.0

Issue Summary

ESP32-S3 features a USB On-The-Go (OTG) interface which complies with the USB 2.0 specification. It supports downloading firmware through USB module. For more information, please refer to Device Firmware Upgrade Through USB. For ESP32-S3 series chips manufactured before Date Code 2219 and modules and development boards with the PW No. before PW-2022-06-XXXX, the **EFUSE_DIS_USB_OTG_DOWNLOAD_MODE (BLK0 B19[7][1])** bit of eFuse is set by default and cannot be modified. Therefore, the USB_OTG Download function is unavailable for these products.

Note: This bit **(BLK0 B19[7])** was defined as **EFUSE_ERR_RST_ENABLE** in previous versions of *ESP32-S3 Technical Reference Manual* and ESP-IDF, and it has been redefined as **EFUSE_DIS_USB_OTG_DOWNLOAD_MODE** in the latest version.

ESP32-S3 also supports downloading firmware through USB_Serial_JTAG. Please refer to Uploading the Application via USB-Serial-JTAG. Users can set **EFUSE_DIS_USB_SERIAL_JTAG_DOWNLOAD_MODE (BLK0 B16[4])** to disable this feature.

Note: This bit **(BLK0 B16[4])** was defined as **EFUSE_DIS_USB_DOWNLOAD** in previous versions of *ESP32-S3 Technical Reference Manual* and ESP-IDF, and it has been updated in the latest version.

[1] BLK0 B19[7]: Indicates the 7th bit of the 19th byte in Block0 of eFuse memory. Similarly hereinafter.

Updates

For ESP32-S3 series chips manufactured on and after Date Code 2219 and modules and development boards with the PW No. of and after PW-2022-06-XXXX, the bit **(BLK0 B19[7])** will be open for users to program since it will not be programmed by default. This will enable the USB_OTG Download function.

EFUSE_DIS_USB_DOWNLOAD_MODE (BLK0 B16[4]) can only be used to disable USB_Serial_JTAG Download. In the latest version of ESP-IDF, it has been renamed **EFUSE_DIS_USB_SERIAL_JTAG_DOWNLOAD_MODE**.

Recommendations for Users

- **Security Recommendations for Using USB_OTG of the ESP32-S3 Series Products After the Updates**

  Recommendations for firmware security–sensitive users:

  1. For ESP32-S3 series products, the USB_OTG Download function will be disabled if any of the **EFUSE_ENABLE_SECURITY_DOWNLOAD**, **EFUSE_DIS_USB_OTG**, or **EFUSE_DIS_DOWNLOAD_MODE** is programmed. In such circumstance, this security advisory can be ignored.

  2. For ESP32-S3 series products manufactured on and after Date Code 2219, if none of the **EFUSE_ENABLE_SECURITY_DOWNLOAD**, **EFUSE_DIS_USB_OTG**, and **EFUSE_DIS_DOWNLOAD_MODE** bits are programmed in the product manufacturing process, users should additionally program the **EFUSE_DIS_USB_OTG_DOWNLOAD_MODE** bit to disable the USB_OTG Download feature during the manufacturing. This will protect the firmware from unauthorized access or malicious attacks via USB_OTG.

- **Security Recommendations for Using USB_Serial_JTAG Download of the ESP32-S3 Series Products After the Updates**

  The **EFUSE_DIS_USB_SERIAL_JTAG_DOWNLOAD_MODE** bit should be programmed separately to protect the firmware from unauthorized access or malicious attacks via USB_Serial_JTAG.

  Note: The bit was defined as **EFUSE_DIS_USB_DOWNLOAD_MODE** previously, but it only disables USB_Serial_JTAG Download. If there is a need to disable USB_OTG Download, please program **EFUSE_DIS_USB_OTG_DOWNLOAD_MODE** according to the above recommendation.

If you need technical assistance, please contact Espressif.