Security Advisory
安全公告

Title/标题	Security Advisory Concerning Partitions Using Flash Encryption 在使用 Flash 加密功能时有关分区加密问题的安全公告
Issue date/发布日期	2021-06-10
Advisory Number/公告编号	AR2021-002
Serial Number/编号	CVE-2021-27926
Version/版本	V1.0

Issue Summary

问题小结

When using the Flash Encryption feature on ESP32 family devices, individual partitions holding data (such as filesystems, custom binary data, etc.) can be marked as encrypted by setting a flag in the ESP-IDF partition table in flash. When this flag is set on a particular partition, all "partition" APIs will transparently decrypt and encrypt data when reading and writing the partition.

在使用 ESP32 系列产品的 Flash 加密功能 时，用户可在 flash 中的 ESP-IDF 分区表将某些分区标记为 "加密"，比如文件系统、定制 bin 数据等。一旦某个分区标记为 "加密"，则全部 "分区" API 在读写这个分区时均会透明地进行数据加解密。

The partition table is also encrypted, but an attacker with physical access may be able to manipulate the partition table ciphertext in flash in order to clear this flag. This will cause the data partition to be treated as plaintext on next boot.

Flash 中的分区表本身也经过加密，但攻击者一旦具备对设备的物理访问权限，则有可能篡改经过加密的分区表，并清除一些分区的 "加密" 标记。这样一来，设备在下次启动时将视这些分区为明文数据来处理。

- This issue does not allow the attacker to read existing encrypted data, but it may allow access to other plaintext values (for example, if the application firmware detects the existing partition contents are now corrupted and writes back default values), or to bypass controls on allowed data (for example, the attacker can write plaintext here and have it read by the application.)

  本问题不会允许攻击者读取已经加密过的数据，但可能对其他明文数据有影响（比如，这可能会导致应用程序固件认为现有分区内容已经损坏，并重新写入默认值），还有可能允许攻击者绕过针对受允许数据的权限控制（比如，攻击者可以在这里篡改受允许的明文数据，然后让应用程序读取这些经过篡改的内容。）

- This issue does not affect data stored using ESP-IDF NVS feature and NVS Encryption, as this feature doesn't rely on the partition encrypted flag.

  由于 ESP-IDF 的 NVS 功能和 NVS 加密过程并不使用分区加密标记，因此不会受到本问题的影响。

- This issue does not affect encrypted application binaries, these are always treated as encrypted data.

  加密的应用程序 bin 文件总是被视为加密数据来处理，因此不会受到本问题的影响。

- This issue does not affect the OTA data partition that controls the currently selected app partition for booting, this partition is always treated as encrypted.

  OTA 数据分区可以控制引导加载程序在启动时应执行哪个应用程序，这个 OTA 数据分区总是被视为加密数据来处理，因此不受本问题的影响。

However:

然而：

- This issue does affect encrypted FATFS partitions when using the ESP-IDF wear levelling feature.

  在使用 ESP-IDF 损耗均衡功能时，本问题会影响加密 FATFS 分区。

- This issue does affect any custom partition API access (functions esp_partition_read, esp_partition_write) when accessing an encrypted partition of a user-defined type.

  在使用客户自定义类型的加密分区时，本问题会影响各种定制分区 API 的使用（esp_partition_read 和esp_partition_write 等功能）

Fixes

修复

This issue can be fixed either by applying an ESP-IDF update, or by adding a check to existing application source code.
本问题可通过升级 ESP-IDF 或增加对现有应用程序源代码的检查来进行修复。

ESP-IDF Fix

ESP-IDF 端修复方法

Updating to the following upcoming ESP-IDF versions will fix the issue. A check for partition table validity is added in these versions, preventing the ciphertext manipulation:
升级至以下即将推出的 ESP-IDF 版本可修复本问题。以下版本增加了对分区表有效性的验证，可防止密文被篡改：

- ESP-IDF master branch after commit 7c11d95a
- ESP-IDF v4.3.1, or release/v4.3 branch after commit a3856c54
- ESP-IDF v4.2.2, or release/v4.2 branch after commit fa734e6a
- ESP-IDF v4.1.2, or release/v4.1 branch after commit 7e0abf78
- ESP-IDF v4.0.3, or release/v4.0 branch after commit bdbfdcdf
- ESP-IDF v3.3.6, or release/v3.3 branch after commit 22487a65

Note: It's only possible to fix this issue via OTA update if the bootloader and partition table were created from ESP-IDF V3.1 or newer, or ESP-IDF V4.0 or newer if using the CMake build system. For installations using bootloader and/or partition table binary generated from ESP-IDF versions older than V3.1, verification of partition table binary is not supported. For these installations, the Application Fix is needed (see below).
注意：仅基于 ESP-IDF V3.1 及以后版本创建的引导加载程序和分区表可通过 OTA 升级来修复本问题。 基于 ESP-IDF V3.1 之前版本创建的引导加载程序和/或分区表，不支持对分区表 bin 文件进行验证。在这种情况下，请参考下方“应用程序端修复方法”。

Application Fix

应用程序端修复方法

It's possible to fix the issue without updating ESP-IDF by adding an application-side check that the "encrypted" flag is set on any data partition that is expected to be encrypted.
如无法升级 ESP-IDF 版本，您也可以在应用程序中增加对分区"加密"标记的检查，确保任何需要加密的分区均已标记 "已加密"。

This check only needs to be performed one time for each partition, after system reset. The partition should be checked before it is first accessed.
每次系统复位后，应在首次访问任何分区前对该分区的 "加密" 标记进行检查，每个分区检查一次即可。

For example, 举例：

```
#include "esp_partition.h"
...
const esp_partition_t *part = esp_partition_find_first(type, subtype, name);
assert(part->encrypted); // note: if assertions are disabled, use a different check.

// ... continue to use 'part'
```

Recommendation for Espressif Devices

其他针对乐鑫产品的推荐做法

- If using flash encryption and storing any data encrypted, verify that the encrypted flag is correctly configured in the partition table.
  在使用 Flash 加密功能和存储任何加密数据时，请总是确保分区表中的 "加密" 标记均已正确设置。

- Immediately update firmware logic to check the "encrypted" flag is set for any partition where it is expected.
  请立即更新固件逻辑，检查任何分区的"加密"标记是否已正确设置。

- Update to an ESP-IDF stable release with the fix, once it becomes available.
  更新至已包含本问题修复的 ESP-IDF 稳定版本（详见上方"ESP-IDF 端修复方法"）。