# 安全公告

| | |
|---|---|
| 标题 | 关于 ESP32 未公开蓝牙命令的补充说明与修复进展 |
| 发布日期 | 2025/05/22 |
| 公告编号 | AR2025-004 |
| 编号 | CVE-2025-27840 |
| 版本 | V1.0 |

## 问题小结

有报道指出，ESP32 蓝牙控制器中存在若干未公开的 HCI 命令。乐鑫此前已澄清，这些厂商自定义 HCI 命令主要用于调试目的，不会带来实质性的、已知的安全威胁。相关技术细节已在我们的一篇博客中进行了说明。

### 影响分析：

在大多数 ESP32 应用场景中，由于蓝牙主机（Host）和控制器（Controller) 都集成在 ESP32 运行的同一个应用程序二进制文件中，因此这些 HCI （ Host Controller Interface ）命令不会带来额外的安全风险。应用程序本身已经拥有对内存和寄存器的完全访问权限，并可自由发送和接收蓝牙数据包，无需依赖这些自定义的 HCI 命令。

这些未公开的 HCI 命令无法通过蓝牙、无线电信号或互联网触发，除非应用本身或无线协议存在漏洞。而如果存在此类漏洞，其影响远大于这些 HCI 命令的存在，且这些命令不会增加额外的攻击面。

在 UART-HCI 模式（ Host-Controller 分离模式）下，ESP32 将蓝牙 HCI 处理任务交由外部主机完成，并默认信任其通过串口接收到的所有 HCI 命令。如果攻击者控制了主机系统，或获取了设备的物理访问权限，则可能向 ESP32 发送未经授权的调试或控制命令，从而改变其行为或暴露数据。然而，这首先需要攻击者成功入侵主机设备或对设备进行物理访问，因此属于第二阶段攻击路径，而非独立的安全漏洞。

### 影响产品系列：

报道中提到的这些“未公开” HCI 命令属于 ESP32 蓝牙控制器 IP 中的调试命令，仅存在于 ESP32 芯片中。而 ESP32-C、ESP32-S 和 ESP32-H 系列芯片的蓝牙控制器并不支持这些命令，因此不受影响。下文所述的修复措施已确保这些调试命令的接口被禁用。

## 应对方法

如前所述，乐鑫已采取以下修复措施：

- 禁用报道中所述的 ESP32 蓝牙控制器中的调试类厂商自定义 HCI 命令接口。
- 提供 API 接口，用于控制是否在最终应用固件中添加乐鑫自有的厂商 HCI 命令——Host-Controller 分离模式使用场景下这些自定义 HCI 命令默认禁用。
- 更新文档，详细说明所有乐鑫自定义的厂商 HCI 命令及其对应的初始化 API。

### ESP-IDF 修复版本：

| ESP-IDF 分支 | 禁用调试类厂商 HCI 命令接口 (Commit ID) | 补充乐鑫自定义 HCI 命令文档 (Commit ID) | ESP-IDF 修复版本 |
|---|---|---|---|
| master | bdd9077b | 16ba8f89 | NA |
| release/v5.4 | 061ba0c9 | daf8117c | v5.4.1 |
| release/v5.3 | efec039d | 07f4ff8c | v5.3.3 |
| release/v5.2 | 72b8f2b5 | a40b0e24 | 预计在 v5.2.6 中修复 |
| release/v5.1 | ff517176 | 1f4106fc | 预计在 v5.1.7 中修复 |
| release/v5.0 | 1f51604a | 87a728c4 | v5.0.9 |

## 给应用程序开发者的建议

建议更新至上述提到的对应 ESP-IDF 版本，以便获得相关修复。