Security Advisory

Title	Security Advisory Follow-Up: Updates and Fixes Regarding ESP32 Undocumented Bluetooth Commands
Issue Date	2025/05/22
Advisory Number	AR2025-004
Serial Number	CVE-2025-27840
Version	V1.0

Issue Summary

A security issue was reported concerning undocumented HCI commands in ESP32 Bluetooth controller. Espressif had earlier clarified that these vendor HCI commands are primarily used for debugging purposes and pose no real, known security threat. Technical details were shared in this blog post.

Impact Analysis:

For the majority of the ESP32 applications, the Bluetooth Host and Controller are part of the same application binary running on ESP32. There is no security risk because the application already has full privileged access to the memory and registers as well as the ability to send/receive Bluetooth packets irrespective of the availability of these HCI commands.

These undocumented HCI commands cannot be triggered by Bluetooth, radio signals, or over the Internet, unless there is a vulnerability in the application itself or the radio protocols. Presence of such vulnerabilities will be a bigger problem, and the presence of these undocumented commands does not offer additional attack surface.

In UART-HCI (hosted) mode, the ESP32 delegates Bluetooth HCI processing to an external host and inherently trusts all commands it receives over the serial interface. Consequently, if an attacker first compromises the host system or gains

physical access to the device, they can issue unauthorized debug or control commands to the ESP32, potentially altering its behavior or exposing data. Because this attack path requires a prior host breach or direct hardware access, it represents a secondary-stage vector rather than a standalone vulnerability.

Affected Product Series:

The "undocumented" HCI commands mentioned in the report are debug commands present in the Bluetooth controller IP in the ESP32. Only the original ESP32 chip has these commands. ESP32-C, ESP32-S and ESP32-H series chips are unaffected as they don't have these commands supported in their Bluetooth controller. The fix described below ensures that the interface to these commands is now disabled.

Precautionary Measures

As per our earlier commitment, we have following measures in place now:

- A fix to disable the interface for debug vendor HCI commands mentioned in the report from ESP32 Bluetooth controller.
- A fix to provide an API interface to control addition of Espressif's own vendor HCI commands in the end application firmware – default disabled for serial HCI use-cases.
- An update to document all Espressif's own vendor HCI commands and their corresponding initialization APIs.

ESP-IDF Patched Versions:

ESP-IDF Branch	Disable debug vendor HCI commands (Commit IDs)	Document Espressif's own vendor HCI commands (Commit IDs)	Fixed ESP-IDF Version
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	Expected in v5.2.6
release/v5.1	ff517176	1f4106fc	Expected in v5.1.7

release/v5.0	1f51604a	87a728c4	v5.0.9

Recommendations for Application Developers

Please consider updating to the corresponding ESP-IDF version highlighted above to take advantage of the fixes.