Security Advisory
安全公告

Title/标题	Security Advisory for Bluetooth Vulnerability 有关蓝牙漏洞的安全公告
Issue date/发布日期	2021-08-31
Advisory Number/公告编号	AR2021-004
Serial Number/编号	CVE-2020-10135 CVE-2020-13595 CVE-2020-26555 CVE-2020-26556 CVE-2020-26557 CVE-2020-26558 CVE-2020-26559 CVE-2020-26560 CVE-2021-28135 CVE-2021-28136 CVE-2021-28139
Version/版本	V1.0

Issue Summary
问题小结

1. Bluetooth® Classic Vulnerabilities reported by Matheus Garbelini for bug bounty. These crashes were divided into 3 classes by Espressif.
   Matheus Garbelini 在 “Bug 悬赏活动”中报告的 Bluetooth® 经典蓝牙漏洞，主要分为三大类：

   - **Class 1 Issues:** CVE-2021-28135 Heap memory was exhausted by flooding LMP packets. Class 1 issues included attacks named:
     第 1 类问题：CVE-2021-28135 LMP 数据包泛洪导致 heap 内存耗尽，包括：

     - Flooding of LMP_au_rand
       LMP_au_rand 泛洪

- Flooding of LMP_features_res
  LMP_features_res 泛洪
- Flooding of LMP_features_req_ext
  LMP_features_req_ext 泛洪

- **Class 2 Issues:** CVE-2021-28136 Function at wrong address was being called which led to InstructionFetchError. Class 3 issues included attacks named:
  第 2 类问题：CVE-2021-28136 调用了地址错误的函数，导致 InstructionFetchError，包括：
  - Crash of duplicated LMP_encapsulated_payload
    重复 LMP_encapsulated_payload 崩溃
  - Crash of wrong LMP_encapsulated_payload
    错误 LMP_encapsulated_payload 崩溃
  - Crash of duplicated LMP_IO_Capability_req
    重复 LMP_IO_Capability_req 崩溃
- **Class 3 Issue:** CVE-2021-28139: Invalid Feature Page Number in LMP_feature_res_ext
  第 3 类问题： CVE-2021-28139 LMP_feature_res_ext 中的 “非法 LMP Feature Page 编号”

2. CVE-2020-13595: HCI Desync
   CVE-2020-13595：HCI 不同步

   In case of abrupt disconnection when sending ACL data, the "Number of Completed Packets" event is incorrectly reported by Bluetooth controller. This can lead to HCI Desync error and result in Bluetooth host stack crash. Fix added to maintain correct number of HCI packets in controller code and send it correctly to host.
   蓝牙控制器在发送 ACL 数据过程中突然被断开连接，会导致蓝牙控制器上报的 "Number Of Completed Packets" 事件错误。这个错误会导致 HCI 不同步，进而导致蓝牙主机协议栈崩溃。通过修复，控制器在这种情况下可以维持正确的 ACL 数据包个数，并将"Number Of Completed Packets" 正确上报给蓝牙主机。

3. CVE-2020-10135: Notification for Bluetooth Impersonation Attacks (BIAS) Vulnerability
   CVE-2020-10135：“蓝牙冒充攻击” (BIAS) 漏洞的通知

VU in Bluetooth Specification announced by Bluetooth SIG. Recommending checks for encryption-type to avoid a downgrade of secure connections to legacy encryption.
这是一个蓝牙联盟组织 （SIG） 公布的蓝牙规范漏洞。建议确认加密类型，避免对端设备将 “仅安全连接” 模式降级为 “传统加密” 模式。

4. CVE-2020-26555: Impersonation in the Pin Pairing Protocol
   CVE-2020-26555：Pin 配对协议中的冒充行为

   VU in Bluetooth Specification announced by Bluetooth SIG. Do not accept connections from or initiate connections to remote devices claiming the same Bluetooth device address as our own.
   这是一个蓝牙联盟组织（SIG）公布的蓝牙规范漏洞。针对声明与我方蓝牙设备地址相同的远程设备，既不要接受也不要发起连接请求。

5. CVE-2020-26556 & CVE-2020-26557:

   a) CVE-2020-26556: Malleable commitment in Bluetooth Mesh Profile provisioning
      CVE-2020-26556：蓝牙 Mesh Profile 配网的 Malleable commitment

   b) CVE-2020-26557: Predictable AuthValue in Bluetooth Mesh Provisioning leads to MITM.
      CVE-2020-26557：蓝牙 Mesh 配网中的 AuthValue 存在可预测性，从而导致中间人攻击

   VU in Bluetooth Specification announced by Bluetooth SIG. AuthValue should be randomly generated with maximum entropy (128-bits) to increase difficulty in brute-force attack. Also, a new AuthValue is selected for each provisioning attempt to increase difficulty in brute-force attack.
   这是一个蓝牙联盟组织（SIG）公布的蓝牙规范漏洞。AuthValue 应采用使用 128 位最大熵生成的随机数，从而提高暴力破解的难度。此外，每次配网都更新 AuthValue， 以增加暴力破解的难度。否则，攻击者可能在离线环境下有足够的时间去破解 AuthValue, 并在下次的配网过程中使用相同的 AuthValue 实现中间人攻击。

6. CVE-2020-26558: Impersonation in the Passkey Entry Protocol
   CVE-2020-26558：Passkey Entry 协议中的冒充行为

   VU in Bluetooth Specification announced by Bluetooth SIG. Reject pairing if the peer public key is same as our own public key.

这是一个蓝牙联盟组织（SIG）公布的蓝牙规范漏洞。如果对方公钥与我方自有公钥相同，则拒绝配对。

7. CVE-2020-26559: Bluetooth Mesh Profile AuthValue leak
   CVE-2020-26559：Bluetooth Mesh Profile AuthValue 泄漏
   VU in Bluetooth Specification announced by Bluetooth SIG. Potentially vulnerable Bluetooth mesh provisioners should use an out-of-band mechanism to exchange the public keys.
   这是一个蓝牙联盟组织（SIG）公布的蓝牙规范漏洞。蓝牙 Mesh 配网者应该使用带外机制交换公钥, 以降低潜在的安全漏洞风险

8. CVE-2020-26560: Impersonation in Bluetooth Mesh Provisioning
   CVE-2020-26560：蓝牙 Mesh 网络配置中的冒充行为
   VU in Bluetooth Specification announced by Bluetooth SIG. Potentially vulnerable Bluetooth mesh provisioners should restrict the authentication procedure and not accept provisioning random and provisioning confirmation numbers from a remote peer that are the same as those selected by the local device.
   这是一个蓝牙联盟组织（SIG）公布的蓝牙规范漏洞。蓝牙Mesh 配网者需要对认证流程加以限制，不应允许使用与自己相同的 Provisioning Random 和 Provisioning Confirmation 值的未配网设备入网，否则会有潜在的安全漏洞风险.

9. ‘Authentication of the Bluetooth LE Legacy Pairing Protocol’ Vulnerability
   “Bluetooth LE Legacy 配对协议认证”漏洞
   VU in Bluetooth Specification announced by Bluetooth SIG. Use Bluetooth LE Secure Connections. Also, where possible, enable and enforce Secure Connections Only Mode.
   这是一个蓝牙联盟组织（SIG）公布的蓝牙规范漏洞。推荐使用 “Bluetooth LE 安全连接”。此外，任何可能情况下，启用并强制执行“仅安全连接”模式。

Patched versions of ESP-IDF

ESP-IDF 修补版本

esp-idf Release	Commit ID
Master	d4232ee8f95a223557e58144cf124fce3280d3ea
release/v4.3	36cb29280aa5e044f5796650e812148f6634b823
release/v4.2	3212d62b2bf5bbfb7d399762770e872478c7ecdd
release/v4.1	bfcaa64b49d70c041e0ae065f597ae9f87601e26

release/v4.0	6ba3ae339b7a4d7bf5a61b9e76d662727848efd7
release/v3.3	35bbd1ba2630c9413386aab456dbdf511e6790ce

Note: Syncing to the commit ids on respective branch will pull all the available fixes
注意：前往相应分支上，进行 commit 同步可拉取所有所需修复。

Recommendations for Espressif Bluetooth® Devices

有关使用乐鑫 Bluetooth® 设备的建议

It is recommended that that:
推荐做法：

- BR/EDR implementations enable Secure Simple Pairing.
  BR/EDR 实施启用“安全简单配对”。

- Bluetooth LE implementations requiring pairing and encryption use Bluetooth LE Secure Connections.
  需要配对和加密的 Bluetooth LE 实现应使用 “Bluetooth LE 安全连接”。

- Where possible, implementations enable and enforce Secure Connections Only Mode, ensuring that Bluetooth LE legacy pairing cannot be used.
  在可能的情况下，实现应启用并强制执行 “仅安全连接”模式，确保无法使用 “传统加密”模式进行配对。

- Bluetooth Mesh Provisioner needs to make sure the Provisioning Random and Confirmation sent and received by itself are not the same.
  蓝牙 Mesh 配网者需要确保自己发送的和从对方设备接收到的 Provisioning Random 和 Provisioning Confirmation 值不同。

- Bluetooth Mesh implementations should enforce a randomly selected AuthValue using all the available bits, where permitted by the implementation. For authentication method, we recommend using Input OOB, which will result in large entropy for the AuthValue.
  在条件允许的情况下，蓝牙 Mesh 实现应强制选择尽可能长的随机 AuthValue 值。推荐使用 Input OOB 进行认证，这可以提高 AuthValue 的熵值。