物聯網設備（低功耗藍牙）保安研究

2020 年 2 月

hkpc 生產力局

HKCERT

免責聲明

香港生產力促進局(生產力局)及轄下香港電腦保安事故協調中心(HKCERT)保留不時修改文件的權利而無須另行通知。

儘管 HKCERT 已盡力確保本文件所含資料均來自可靠來源，但對任何錯誤或遺漏或使用相關資料所招致的結果概不負責。 本文件上的所有資料均以當時情況提供，不擔保其完整性、準確性、及時性、或使用相關資料所招致的結果，亦不作任何明示或隱含的保證，包括但不限於其性能保證、適售性和特定用途的適用性。

本文件包含的資料僅供參考。 信賴或使用相關資料由讀者自行承擔風險。 本文件的任何內容均不得在任何程度上替代讀者的獨立調查和合理的技術和商業判斷。 在任何情況下，HKCERT、生產力局、或其合作夥伴、員工或代理商，均不對你或任何人信賴本文件相關資料做出的任何決定或行動，或任何後果性，特殊或類似的損害承擔責任。

版權

目錄

1. 背景

隨著無線技術的迅速發展，物聯網的應用越來越廣泛，而物聯網設備亦因應其應用需要採用合適的無線技術。其中，低功耗藍牙技術具備低功耗、價廉及易於應用等優點，成為物聯網設備使用最多的無線技術之一，在家居、健康、娛樂、工業等領域均有應用。

低功耗藍牙設備一方面為大眾帶來便利，但另一方面其技術的保安漏洞亦會帶來危險。攻擊者可能會試圖控制設備，從設備中竊取敏感資訊，遠程執行程式碼，甚至造成其他實質損害。

同時，低功耗藍牙設備亦涉及私隱問題，存在設備被追蹤的可能性。

因此，HKCERT 針對一些低功耗藍牙設備進行了保安測試及研究，期望透過測試結果闡述有關保安問題，幫助開發人員及一般用戶提高對低功耗藍牙設備的安全意識。

2. 低功耗藍牙設備保安研究

低功耗藍牙的使用，既讓物聯網設備更方便使用，又使設備與應用之間的連接更簡單快捷。

由於低功耗藍牙晶片價格相宜和易於應用，所以不同類型的家居電器都會加入低功耗藍牙晶片，以便能簡單地連接手機應用程式，進行操作和特定配置，以方便使用和改善用戶體驗。

低功耗藍牙在醫療健康設備中的應用亦相當普遍；因為其晶片體積小、功耗低，廠家能夠設計出不同可穿戴裝置，例如加入感應器的智能手環，監測健康狀態。這些設備僅依靠一個微小的電池便能運作數月或數年，大大減少更換電池的頻率。用戶購買這類可穿戴裝置，連接手機應用程式，便能隨時監測健康狀況。

2.1 三類攻擊方式及其特點

儘管低功耗藍牙設備為用戶帶來更多便利，但與此同時，不正確的低功耗藍牙配置亦會引發保安問題，有機會讓攻擊者乘虛而入。低功耗藍牙的攻擊主要有三類：被動攻擊、主動攻擊、身份追蹤，具體見下表。

攻擊方式	**攻擊特點**
被動攻擊	被動式竊聽設備間的數據傳輸，以獲取傳輸中的資料及操作命令。
主動攻擊	主動向目標設備發送數據或作為中間人篡改數據，使設備接收錯誤數據或運行非法操作命令。
身份追蹤	通過掃描和收集藍牙設備地址，繪製設備運作的軌跡，以找出持有這些設備的用戶，掌握他們的行蹤及習慣等。

2.2 應用類型及防禦

由於低功耗藍牙設備的應用各有不同，因此它們的保安配置亦要配合硬件限制和保安需求，而設備生產商可以根據應用的特徵，選擇正確的保安配置來防禦攻擊。

以下圖表是 HKCERT 建議的需要配置保安配置的應用類型、設備範例和需要防禦的攻擊類型：

應用類型	**設備範例**	**需要防禦的攻擊類型**
設備需要傳輸敏感資料	通訊設備、關鍵設備傳感器等	被動攻擊
設備如果被非法操作會影響人身或者環境安全	家居電器、醫療健康設備、運輸設備、工業操作設備等	主動攻擊
設備需要隨身携帶	可穿戴設備，移動設備	身份追蹤

譬如通訊設備需要傳輸敏感資料，因此會建議設備採取防禦被動攻擊的保安配置，以免被竊取傳輸中的資料。至於會導致設備運行非法操作命令，有機會危及人身或環境安全的攻擊，必須採用可以防禦主動攻擊的保安配置。此外，隨身攜帶的設備則要避免身份追蹤或泄露用戶行蹤。

如果一個設備同時有以上多個特點，例如隨身的醫療健康設備，既需要隨身亦可能影響人身安全，就需要使用防禦主動攻擊和身份追蹤的保安配置。

低功耗藍牙有多種相應的保安配置來防禦以上提及的攻擊，包括配對加密(針對主動和被動攻擊)和私隱保護(針對身份追蹤)功能。以下會簡單介紹配對加密和私隱保護保安功能，同時我們亦對低功耗藍牙設備在這兩方面的保安程度進行了調查。

3. 低功耗藍牙的配對加密保安程度介紹及分析

3.1 配對加密介紹

低功耗藍牙設備需要配對方能建立連接，有兩種不同的配對方法，分爲 LE 傳統配對和 LE 安全連接配對（藍牙 4.2 或之後版本適用）。LE 安全連接配對使用 Elliptic curve Diffie–Hellman (ECDH)生成密鑰來加密連接，比傳統配對更安全，可以有效防禦被動攻擊。

而傳統配對有三種配對方式：Just Works，Passkey Entry，Out Of Band (OOB)，LE 安全連接配對比傳統配對增加 Numeric Comparison 配對方式。以下圖表是各種配對方式的特徵及保安程度：

配對方式	LE 傳統配對	LE 安全連接配對	配對特徵	適用範圍	保安程度
Just Works	✓	✓	無需用戶動作。	無顯示，無輸入的設備。	LE 傳統配對模式無法防禦被動及主動攻擊。 LE 安全連接配對模式可防禦被動攻擊，無法防禦主動攻擊。
Passkey Entry	✓	✓	需要用戶輸入 6 位 PIN 碼驗證。	發起連接的設備需要有輸入，被連接的設備需要有顯示。	LE 傳統配對模式可防禦主動攻擊。因為密鑰可被暴力破解，無法完全防禦被動攻擊。 LE 安全連接配對模式可防禦被動及主動攻擊。
Out Of Band	✓	✓	使用藍牙以外的無綫技術配對（如 NFC）。	有藍牙以外的無綫技術（如 NFC）的設備。	LE 傳統配對模式及 LE 安全連接配對模式皆可防禦被動及主動攻擊。
Numeric Comparison	✗	✓	需要用戶確認兩個設備顯示的 6 位數字是否相同。	有顯示及確認/取消輸入的設備。	LE 安全連接配對模式可防禦被動及主動攻擊。

就章節 2.2 提及的三種應用類型，HKCERT 建議開發人員參考以下準則配置相應保安程度的配對加密方式：

- 傳輸敏感資料的設備，要防禦被動攻擊，所以要選擇 LE 安全接連配對，如使用 LE 傳統配對，則採用 Out Of Band 配對方式。
- 非法操作會影響人身或者環境安全的設備要防禦主動攻擊，則要應用 Passkey Entry、Out Of Band 或者 Numeric Comparison 配對方式。
- 若設備不會影響人身或環境安全，或者無顯示及輸入，可使用 Just Works 配對方式，建議廠商使用 LE 安全連接配對，同時設置藍牙開關，不使用藍牙時可關閉藍牙避免主動攻擊。

3.2 保安程度分析

我們就低功耗藍牙設備的配對加密保安程度進行調查，結果發現部分低功耗藍牙設備並沒有使用正確的配對加密方式，被黑客攻擊會造成實質損害。

例如，我們在一款可用低功耗藍牙連接的智能直髮電器產品，發現它雖然有電子顯示屏，但使用的卻是 LE 傳統配對的 Just Works 配對方式，並且無獨立的藍牙開關。我們亦透過測試平臺竊聽傳輸數據，找到調整溫度和發熱時間的操作值，然後通過主動連接設備寫入對應數值改變溫度和發熱時間。此外，我們也可以進行中間人攻擊，篡改使用者對直髮器的操作指令。這個保安漏洞會導致直髮器被設定於錯誤的溫度和發熱時間，譬如被設定在最高溫度攝氏 235 度發熱 20 分鐘，並放在易燃物品旁，可能會引發火警。

若該款產品被非法操作，有可能危及人身或環境安全，所以應該採用防禦主動攻擊的配對加密方式；而此產品有顯示輸出，廠商應該選擇 Passkey Entry 配對方式，而不是 Just Works 配對方式。由此可見，沒有使用正確的配對加密方式，將大大增加設備被成功攻擊的風險，並有機會危及人身或環境安全。

詳細測試細節可參考章節 7.1。

4. 低功耗藍牙的私隱保護保安程度介紹及分析

4.1 私隱保護介紹

藍牙設備起用稱為藍牙設備位址（BD_ADDR）的位址作為識別字。當藍牙設備在閒置狀態，會向外廣播該地址供其他設備連接，當建立連接後，該地址會作爲接受及發送數據的地址。這存在著私隱風險，因為攻擊者可以透過過掃描和收集藍牙設備地址，繪製設備活動的足跡，藉以推斷和掌握設備用戶的行蹤和習慣。

藍牙的私隱保護功能旨在減低這種風險。使用隱私保護功能時，設備具有兩個位址。第一個是身份位址，它用作藍牙設備的不變識別字。第二個是私有設備位址，該位址會定期更改。私有位址掩蓋設備的身份，在使用中，通過無線資料包公開發送的是私有位址，而不是身份地址。

4.2 保安程度分析

我們測試發現有隨身攜帶的低功耗藍牙設備，譬如智能手環，並沒有使用藍牙私隱保護功能，其藍牙設備地址不會定期更改。假如用戶設定智能手環署上自己的名字，設備名變爲「某某的手環」，智能手環向外廣播的數據中又包含設備名，攻擊者就可以掌握到該用戶的名字及行蹤，可能會對用戶推送廣告或者利用資訊進行詐騙。

詳細測試細節可參考章節 7.2。

5. 建議

5.1 一般用戶

- 應該透過官方渠道購買低功耗藍牙設備，購買前搜尋該低功耗藍牙設備是否有保安漏洞、官方網站是否提供韌體更新等資訊；
- 使用低功耗藍牙設備時才開啓，並於開啓后立即連接設備，設備閒置時便需關閉；
- 定期檢查並更新設備的韌體；以及
- 避免在藍牙設備名稱上設置有關個人私隱的訊息 (例如: 姓名、ID、電話號碼等)。

5.2 產品開發人員

- 可利用 HKCERT 的《物聯網保安最佳實踐指引》4.2.4.1 無綫安全的自我評估清單，加强產品保安；
- 根據產品特性，選擇建議的保安配置(詳情請考章節 5.3 的表格) ；以及
- 及時推出修補低功耗藍牙產品漏洞的韌體更新。

5.3 根據產品特性和應用類型的保安配置建議

- 一般用戶與產品開發人員可參考以下準則購買或開發低功耗藍牙設備。

應用類型	設備範例	需要防禦的攻擊類型	保安配置建議
設備需要傳輸敏感資料	通訊設備、 關鍵設備傳感器等	被動攻擊	選擇 LE 安全接連配對，如只能選取 LE 傳統配對，需使用 Out Of Band 配對方式。
設備如被非法操作，會影響人身或者環境安全	家居電器、 醫療健康設備、 運輸設備、 工業操作設備等	主動攻擊	選擇 Passkey Entry，Out Of Band 或者 Numeric Comparison 配對方式。
設備不會影響人身或者環境安全，或者無顯示及輸入	無傷害性的娛樂應用設備	無	建議使用 LE 安全連接配對的 Just Works 配對方式，同時提供藍牙開關功能，以便用戶在不需要藍牙操作時關閉藍牙訊號。
設備需要隨身攜帶	可穿戴設備、 移動設備	身份追蹤	藍牙設備地址應該啓用私隱保護功能令藍牙私有地址定

			期更改，避免設備被追蹤，泄漏用戶私隱。

6. 總結

- 低功耗藍牙設備未來數年會繼續增長，針對有關設備的網絡攻擊亦會隨之增加。
- 開發者應該根據產品應用特徵，為低功耗藍牙設備選擇正確的配對加密方式，防禦被動及主動攻擊。
- 傳輸敏感資料的設備，要防禦被動攻擊，防止被竊聽造成數據泄露。
- 涉及人身和環境安全的低功耗藍牙設備若遭受主動攻擊，或可能造成實質損害。
- 隨身的低功耗藍牙設備有可能被追蹤，應啓用私隱保護功能。
- 開發者可使用《物聯網保安最佳實踐指引》對產品做自我評估，加强產品保安。

7. 附錄

7.1 直髮電器產品保安測試

我們對一款使用低功耗藍牙的直髮電器產品進行保安測試。

這款直髮器除了利用實體按鈕操作外，還附帶藍牙無線設備，讓用戶透過手機應用程式進行遙距操作。我們的測試主要分為竊聽數據及主動攻擊，測試的流程可參考以下攻擊流程示意圖。

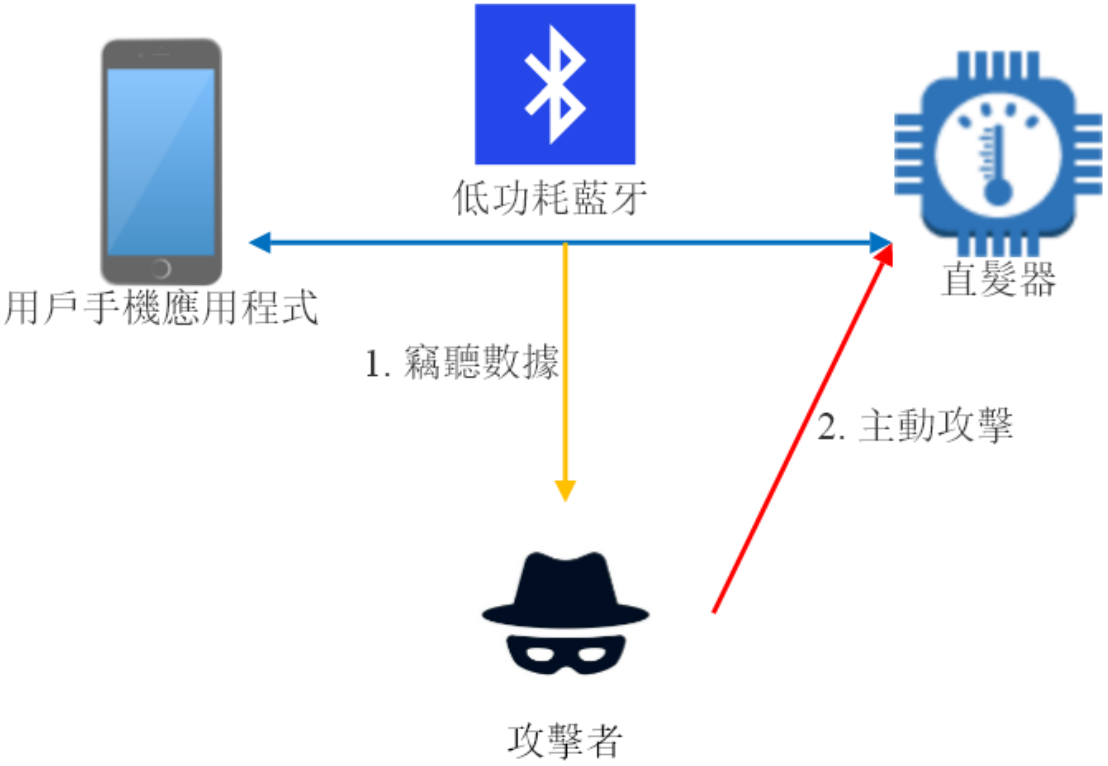

Fig. 7.1.1 攻擊流程示意圖

啓動直髮器後，我們使用測試平臺對附近的藍牙設備進行掃描，發現這款直髮器能被掃描出。

Fig. 7.1.2 藍牙設備參數的掃描結果

調查直髮器的 GATT 檔案後，發現操作值為 0015 這一項有寫入權限，表示可通過寫入數值來控制直髮器。

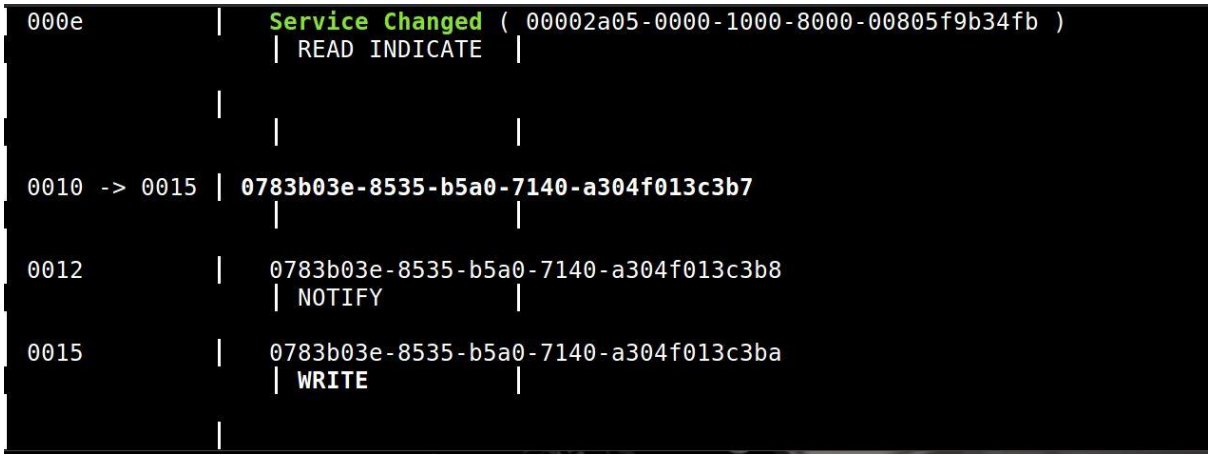

Fig. 7.1.3 藍牙設備操作值的讀寫權限

我們通過截取直髮器與控制的應用程式之間的通訊，推斷出控制直髮器動作的數值。

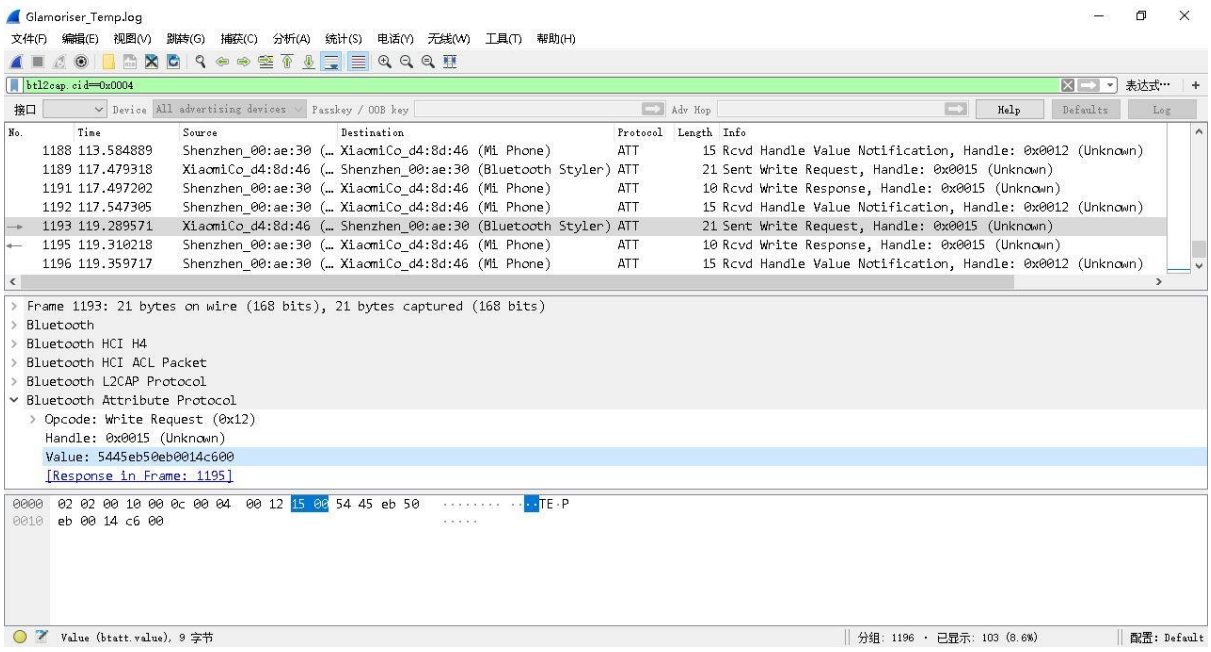

Fig. 7.1.4 藍牙設備與應用程式之間通訊的原始內容

我們通過測試平臺把代表溫度攝氏 235 度的數值，寫入對應的操作值。

```
[    ][f0:13:c3:00:ae:30][LE]> connect
[CON][f0:13:c3:00:ae:30][LE]> char-write-req 0015 5445eb50eb0014c600
[CON][f0:13:c3:00:ae:30][LE]> Characteristic value was written successfully
```

Fig. 7.1.5　寫入藍牙設備對應的 Handle 值

直髮器初始溫度為攝氏 80 度。

Fig. 7.1.6　寫入操作值前直髮器的初始溫度

接收到指令後，直髮器升高到攝氏 235 度。

Fig. 7.1.7 寫入操作值後直髮器改變溫度

該款直髮器發熱時間最長可設置為 20 分鐘，如果被設置為攝氏 235 度，擺放在易燃物品旁，極有可能引起火災。

我們使用 HKCERT 的《物聯網保安最佳實踐指引》4.2.4.1 無綫安全中的自檢表對該產品的低功耗藍牙傳輸安全性進行評估。

無綫安全自我評估清單

自我評估項目	評估結果
☐ 在全部無綫通訊過程中啓用加密。	**無。**該產品配對加密方式是 LE 傳統配對的 Just Works，無法防竊聽，相當於無加密。該產品無傳輸敏感資料，可以不使用加密來防禦被動攻擊。但攻擊者會通過被動攻擊獲取到操作的指令，從而逆向分析指令格式，所以建議使用 LE 安全連接配對防禦。
☐ 儘管無綫協議沒法提供加密功能，數據在傳輸前在應用層就被加密。	**無。**該產品數據在應用層不會加密，並且控制動作的數值是固定的。 該產品無傳輸敏感資料，可以不使用加密來防禦被動攻擊。但攻擊者會通過被動攻擊獲取到操作的指令，從而逆向分析指令格式，如果在連接層不使用加密的情況下，建議在應用層加密。
☐ 由於設備計算能力有限，因此仍可以使用替代的加密方法來確保無線數據流中的內容免遭竊聽。	**無。**該產品配對加密方式是 LE 傳統配對的 Just Works，無法防竊聽。 可以使用以上提供的兩種方式加密防止竊聽。
☐ 初始配對過程中需要用戶交互，以避免與未授權的第三方配對。	**無。**該產品配對加密方式是 LE 傳統配對的 Just Works，配對過程不需要用戶交互。 該產品會因爲非法操作而導致人身或環境安全收到損害，所以一定要防禦未授權的第三方的主動攻擊。配對過程需要用戶交互，因爲該產品有電子顯示屏，建議使用 Passkey Entry 配對方式。
☐ 默認的無線密碼僅在初始配對過程中使用一次，並為繼續正常服務需要被強制更改。	不適用。

就以上評估結果可見，如該款產品能採納指引的最佳實踐項目，可以有效地改善有關產品的無綫安全。

7.2 智慧手環私隱保安測試

我們對一款使用低功耗藍牙的智能手環產品的私隱保安進行測試。

我們發現該手環沒有啓用私隱保護功能，藍牙設備位址不會定期更改。如果用戶在設備名設定中含有用戶的名字，攻擊者可以通過掃描及收集藍牙設備地址，生成設備運作的軌跡，掌握用戶的行蹤及習慣等。

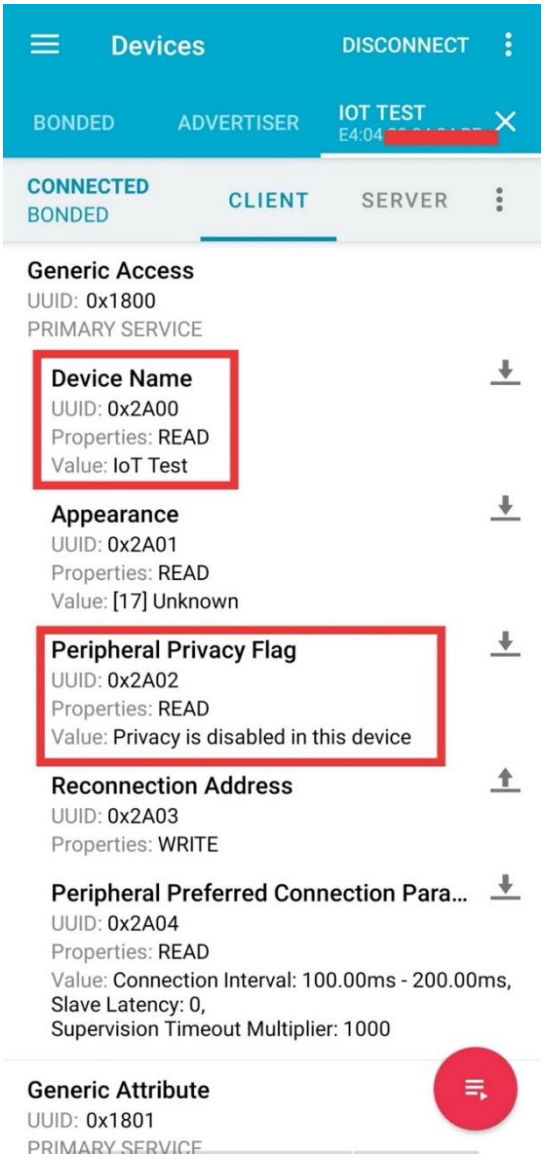

Fig. 7.2.1 智能手環私隱保安配置問題