Một số vấn đề về khả năng rò rỉ thông tin người dùng của ứng dụng Bluezone ở những phiên bản đầu tiên ra mắt.

*/ Việc gán ID cố định cho mỗi bản cài đặt:

- bluezone gán cho mỗi bản cài đặt 1 ID cố định dựa trên thời gian ứng dụng được cài đặt trên ứng dụng.
- khả năng bị rò rỉ các thông cá nhân mang tính nhạy cảm: vị trí, lịch trình di chuyển .v..v.
- sự nhầm lẫn về việc địa chỉ MAC là cố định mà team đưa ra về việc thay đổi ID là không cần thiết.

+ Bluetooth Classic
    - discoverable, thiết bi sẽ phát (địa chỉ MAC, tên thiết bị và các thông tin khác)
    - non-discoverable, thiết bị không phát gì.

+ Bluetooth Low Energy
    - android sẽ thay đổi địa chỉ MAC mỗi khi nó được khởi động.
    - ios thay đổi địa chỉ MAC ngẫu nhiên theo 1 khoảng thời gian.

Phần mã code tạo ID cho người dùng

```
var generateUserId = function () {
    var t = '0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ',
        n = t.length,
        o = '';
    Math.seedrandom(new Date().getTime());
    for (var s = 0; s < 6; s++) o += t.charAt(Math.floor(Math.random() * n));
    return o;
 }
```

- Những khả năng tiềm ẩn mà cộng đồng đưa ra về việc thông tin người dùng bị rò rỉ:

    + Kẻ tấn công có thể tạo ra tất cả các ID có thể và phát đi khắp nơi, có thể nhắm mục tiêu một nhóm người dùng mà đã cài đặt ứng dụng trong một số khung thời gian cụ thể. Sau khi tạo ID, ứng dụng sẽ đăng ký ID đó với máy chủ. Nó tạo mã thông báo FCM và liên kết ID với mã thông báo.

    + Cộng đồng cho rằng máy chủ sử dụng điều này để gửi ID bị nhiễm bệnh và các thông báo khác tới ứng dụng. Nếu đăng ký không thành công vì ID đã tồn tại, ứng dụng sẽ không tạo ID khác và sẽ thử lại. Vì ta có thể dự đoán tất cả các ID trong tương lai và có thể đăng ký trước tất cả chúng. Đây là một cuộc tấn công từ chối dịch vụ, từ chối tất cả người dùng trong tương lai tham gia vào hệ thống.

- Người dùng có thể tấn công và chỉnh sửa kết quả lây nhiễm:

    + Nếu cơ sở dữ liệu dự phòng được cơ quan y tế sử dụng để xác định ai sẽ cách ly, người dùng có thể dễ dàng làm sai lệch hồ sơ phơi nhiễm. Vì Ứng dụng sao lưu vào bộ nhớ chung của Android (còn gọi là bộ nhớ ngoài) cơ sở dữ liệu của tất cả các

ID được quan sát và địa chỉ MAC cũng như tên thiết bị của các thiết bị Bluetooth Classic.

***/ ID quá ngắn**

- Cộng đồng cho rằng ID cố định mà mỗi người dùng được cấp khi cài đặt ứng dụng là quá ngắn. Tất cả chỉ có khoảng 36^6 ~ 2^31 ID. Do nghịch lý ngày sinh (birthday paradox), nếu 65 nghìn người sử dụng ứng dụng, hai người trong số họ sẽ được chỉ định cùng một ID với xác suất cao. Khi đó, nếu một người được tuyên bố là bị nhiễm bệnh, thì người kia cũng vậy.

*/ Ứng dụng yêu cầu quyền truy cập vào external storage

- external storage là nơi chứa các thông tin nhạy cảm như: lưu trữ ảnh, phương tiện và tệp.