BỘ CÔNG AN
CÔNG AN TỈNH THÁI NGUYÊN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 269 /CAT-PA05

Thái Nguyên, ngày 15 tháng 7 năm 2025

V/v cảnh báo lỗ hổng bảo mật tấn công mạng thông qua kết nối bluetooth của các phương tiện ô tô

Kính gửi:
- Các sở, ban, ngành, đoàn thể thuộc tỉnh;
- UBND các xã, phường.

Qua công tác bảo đảm an toàn, an ninh mạng, Công an tỉnh Thái Nguyên phát hiện lỗ hổng bảo mật "Perfektblue" khai thác thông qua kết nối bluetooth trên các phương tiện ô tô, có khả năng đánh cắp các dữ liệu cá nhân nhạy cảm và thực thi mã độc từ xa được công khai trên không gian mạng. Cụ thể như sau:

Kẻ tấn công có thể khai thác các lỗ hổng này khi ở trong phạm vi gần phương tiện ô tô và ghép nối thiết bị của đối tượng với hệ thống thông tin giải trí của xe qua Bluetooth. Nếu thành công, kẻ tấn công có thể theo dõi vị trí, tọa độ của phương tiện (GPS), đánh cắp dữ liệu ghi âm các cuộc gọi, tin nhắn và các dữ liệu hệ thống, dữ liệu cá nhân nhạy cảm khác được lưu trữ trên thiết bị màn hình điều khiển có kết nối bluetooth của phương tiện ô tô.

Các thiết bị ảnh hưởng trực tiếp bởi lỗ hổng bảo mật này là hệ thống màn hình điều khiển, giải trí của các xe ô tô. Đặc biệt là các sản phẩm của bên thứ 3, không phải thiết bị được lắp đặt chính hãng. Để khai thác lỗ hổng bảo mật này, kẻ tấn công sẽ tiếp cận phương tiện ô tô của bị hại, sau đó ghép nối thiết bị cài đặt công cụ tấn công với thiết bị của ô tô thông qua kết nối bluetooth. Khi kết nối thành công, đối tượng sẽ có quyền truy cập và có thể thực thi một số mã độc từ xa (RCE) để lấy cắp dữ liệu, điều chỉnh các thông số hệ thống. Nghiêm trọng hơn, một số phương tiện ô tô hiện đại có các chức năng điều khiển an toàn, điều khiển tự động có thể bị đối tượng thay đổi các cài đặt, gây ảnh hưởng đến hoạt động bình thường của các chức năng điều khiển phương tiện, tiềm ẩn nguy cơ mất an toàn khi tham gia giao thông.

(Có phụ lục thông tin chi tiết và hướng dẫn phòng ngừa hoạt động tấn công kèm theo)

Từ tình hình trên, Công an tỉnh đề nghị các sở, ban, ngành, tổ chức chính trị xã hội của tỉnh, UBND xã, phường phối hợp triển khai một số nội dung sau:

1. Cảnh báo đến cán bộ, công chức, viên chức, người lao động tại đơn vị và người dân sinh sống trên địa bàn về lỗ hổng bảo mật này và phổ biến cách

thức phòng ngừa (tại phụ lục kèm theo văn bản), đặc biệt là đối với các đồng chí lãnh đạo, người đứng đầu cơ quan, đơn vị cần quan tâm nâng cao cảnh giác khi di chuyển, công tác bằng phương tiện ô tô.

2. Tiếp tục phối hợp với Công an tỉnh trong công tác bảo đảm an ninh mạng, an toàn thông tin. Quá trình thực hiện nếu gặp khó khăn, vướng mắc hoặc trường hợp ghi nhận, phát hiện phương tiện bị tấn công từ xa, đề nghị trao đổi ngay với Công an tỉnh (qua Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Đ/c Trung úy Nguyễn Anh Tuấn, SĐT: 0977.721.841) để phối hợp xử lý.

Công an tỉnh thông báo để các cơ quan, đơn vị, địa phương phối hợp thực hiện./.

Nơi nhận:
- Như trên: Phối hợp thực hiện;
- Đ/c Chủ tịch UBND tỉnh: Báo cáo;
- Đ/c Giám đốc CAT: Báo cáo;
- Phòng PH10, PC08, PV01: Theo dõi;
- Lưu VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG AN TỈNH THÁI NGUYÊN

Đại tá Thăng Quang Huy

PHỤ LỤC

Thông tin chi tiết về lỗ hổng bảo mật "Perfektblue" và cách thức phòng ngừa hoạt động tấn công

(Kèm theo công văn số 269 /CAT-PA05 ngày 15 /7/2025)

1. Thông tin về lỗ hổng bảo mật

"PerfektBlue" là một trong bốn lỗ hổng bảo mật nghiêm trọng trong ngăn xếp Bluetooth BlueSDK của OpenSynergy, được phát hiện bởi PCA Cyber Security. Những lỗ hổng này có thể cho phép thực thi mã từ xa (RCE) trên hàng triệu phương tiện từ các nhà cung cấp như Mercedes-Benz, Volkswagen và Skoda.

Kẻ tấn công có thể khai thác các lỗ hổng này khi ở trong phạm vi gần xe và ghép nối thiết bị của họ với hệ thống thông tin giải trí của xe qua Bluetooth. Nếu thành công, kẻ tấn công có thể theo dõi tọa độ GPS, ghi âm, truy cập danh bạ và có khả năng kiểm soát các chức năng phần mềm quan trọng của xe, bao gồm cả động cơ.

Phạm vi ảnh hưởng: Lỗ hổng này có khả năng ảnh hưởng đến hàng triệu phương tiện giao thông.

Hệ thống mục tiêu: Các lỗ hổng này nhắm vào hệ thống thông tin giải trí trong xe (IVI - In-Vehicle Infotainment system) thông qua Bluetooth.

Điều kiện để khai thác lỗ hổng:

- **Trong phạm vi gần:** Kẻ tấn công phải ở trong phạm vi tối đa 5 - 7 mét so với ô tô.
- **Xe bật khóa điện:** Xe phải đang ở trạng thái bật khóa điện.
- **Chế độ ghép nối Bluetooth:** Hệ thống thông tin giải trí trong xe phải đang ở chế độ ghép nối (pairing mode).
- **Người dùng chấp thuận:** Người dùng xe phải chủ động chấp nhận kết nối Bluetooth bên ngoài từ kẻ tấn công trên màn hình.
- **Duy trì khoảng cách:** Kẻ tấn công phải duy trì khoảng cách gần (5-7 mét) để giữ quyền truy cập, do giới hạn về khoảng cách của Bluetooth.

2. Cách thức phòng ngừa:

- **Không chấp nhận ghép nối lạ:** Đây là nguyên tắc quan trọng nhất. Nếu hệ thống thông tin giải trí trên xe hiển thị yêu cầu ghép nối Bluetooth từ một thiết bị không quen thuộc, tuyệt đối không chấp nhận. Kẻ tấn công cần sự chấp thuận của bị hại để thiết lập kết nối.
- **Tắt Bluetooth khi không sử dụng:** Nếu không có nhu cầu sử dụng Bluetooth (ví dụ: không nghe nhạc qua điện thoại, không gọi điện), cần tắt tính năng Bluetooth trên hệ thống thông tin giải trí của xe. Điều này giúp giảm thiểu "bề mặt tấn công" mà kẻ xấu có thể nhắm tới.

- **Xóa thiết bị đã ghép nối không dùng đến:** Định kỳ kiểm tra danh sách các thiết bị đã ghép nối trong cài đặt Bluetooth của xe và xóa bỏ những thiết bị mà không còn sử dụng hoặc không nhận ra.

- **Sử dụng tên thiết bị duy nhất:** Khi ghép nối điện thoại với xe, cần đặt tên Bluetooth cho điện thoại thật cụ thể và dễ nhận biết để tránh nhầm lẫn với các thiết bị lạ xung quanh.