BỘ CÔNG AN
CÔNG AN TỈNH THÁI NGUYÊN

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

Số: 147 /CAT-PA05

Thái Nguyên, ngày 12 tháng 01 năm 2026

V/v cảnh báo nguy cơ tấn công mạng thông qua khai thác lỗ hổng thiết bị định tuyến (router) đã hết vòng đời hỗ trợ

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

Qua công tác nắm tình hình trên không gian mạng, Công an tỉnh phát hiện nguy cơ tấn công mạng nghiêm trọng xuất phát từ việc khai thác lỗ hổng trên các thiết bị định tuyến (router) đời cũ, đã hết vòng đời hỗ trợ và đang được tin tặc lợi dụng làm cửa ngõ xâm nhập từ xa vào hệ thống mạng nội bộ của cơ quan, tổ chức, cụ thể:

Nhiều mẫu router D-Link[1] đời cũ tồn tại lỗ hổng bảo mật được gán mã CVE-2026-0625, thuộc nhóm command injection, cho phép thực thi lệnh từ xa mà không cần xác thực. Lỗ hổng nằm trong thành phần cấu hình DNS của thiết bị, cho phép đối tượng tấn công chèn và thực thi lệnh hệ thống trực tiếp thông qua giao diện quản trị, trong một số trường hợp không cần đăng nhập. Đáng chú ý, các thiết bị bị ảnh hưởng đều đã ngừng được nhà sản xuất hỗ trợ từ nhiều năm trước, không còn bản vá bảo mật, khiến nguy cơ bị khai thác tồn tại lâu dài và không thể khắc phục triệt để bằng các biện pháp kỹ thuật thông thường.

Việc router bị chiếm quyền kiểm soát có thể dẫn đến các hậu quả đặc biệt nghiêm trọng, bao gồm:

- Đối tượng tấn công kiểm soát toàn bộ luồng dữ liệu ra/vào mạng nội bộ;
- Theo dõi, thu thập, chuyển hướng hoặc đánh cắp dữ liệu của các hệ thống phía sau;
- Cài đặt mã độc, biến thiết bị thành một phần của botnet;
- Sử dụng router làm bàn đạp để xâm nhập sâu vào các máy chủ, máy trạm và hệ thống thông tin nội bộ;
- Gây nguy cơ lộ, mất thông tin nội bộ, thông tin nhạy cảm, thậm chí bí mật nhà nước.

Đây là nguy cơ đặc biệt nguy hiểm do thiết bị mạng đóng vai trò trung

[1] Các thiết bị router D-Link bị ảnh hưởng bao gồm: DSL-526B (≤ 2.01), DSL-2640B (≤ 1.07), DSL-2740R (< 1.17), DSL-2780B (≤ 1.01.14)

tâm trong hạ tầng công nghệ thông tin. Khi bị xâm nhập, toàn bộ hệ thống phía sau có thể bị kiểm soát mà người quản trị không phát hiện, nhất là trong các cơ quan, đơn vị chưa tổ chức rà soát, thay thế thiết bị mạng cũ.

Trước tình hình trên, Công an tỉnh kiến nghị các cơ quan, đơn vị, địa phương khẩn trương triển khai thực hiện các nội dung sau:

1. Rà soát, thống kê toàn bộ các thiết bị mạng đang sử dụng, đặc biệt là router, modem, firewall tại trụ sở làm việc, đơn vị trực thuộc; kịp thời phát hiện các thiết bị đã hết vòng đời hỗ trợ, tiềm ẩn nguy cơ mất an toàn thông tin.

2. Khẩn trương thay thế các thiết bị mạng đã hết vòng đời hỗ trợ, không còn được nhà sản xuất vá lỗi bảo mật; không tiếp tục sử dụng các thiết bị tồn tại lỗ hổng nghiêm trọng không thể khắc phục.

3. Chỉ đạo bộ phận, cán bộ quản trị hệ thống mạng tại cơ quan, đơn vị: (1)Tuyệt đối không bật chức năng quản trị thiết bị mạng từ xa qua Internet khi không thực sự cần thiết; trường hợp bắt buộc phải sử dụng, cần áp dụng các biện pháp kiểm soát chặt chẽ, phân vùng mạng và giám sát truy cập. (2)Tăng cường giám sát an ninh mạng tại lớp hạ tầng, theo dõi các dấu hiệu bất thường liên quan đến truy cập trái phép, thay đổi cấu hình DNS, lưu lượng mạng bất thường. (3)Khi phát hiện thiết bị mạng có dấu hiệu bị xâm nhập, bị thay đổi cấu hình trái phép hoặc nghi ngờ bị khai thác lỗ hổng, phải coi đây là sự cố an ninh mạng nghiêm trọng, khẩn trương cô lập thiết bị, bảo toàn dữ liệu và thông báo ngay cho Công an tỉnh (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để phối hợp xử lý theo quy định.

Quá trình thực hiện nếu gặp khó khăn, vướng mắc hoặc trường hợp ghi nhận, phát hiện hệ thống thông tin của đơn vị bị tấn công mạng, 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).

Công an tỉnh đề nghị các cơ quan, đơn vị, địa phương nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên: Phối hợp thực hiện;
- Đ/c Giám đốc CAT: Báo cáo;
- Phòng PV01: Theo dõi;
- Lưu VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG HOÀ X.H.C.N VIỆT NAM
CÔNG AN TỈNH THÁI NGUYÊN

Đại tá Thăng Quang Huy