BỘ CÔNG AN
CÔNG AN TP HÀ NỘI

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

Số:3469 /CAHN-ANM&PCTPSDCNC
V/v cảnh báo một số lỗ hổng bảo mật nguy hiểm trên thiết bị mạng, phần mềm

Hà Nội, ngày 19 tháng 05 năm 2026

Kính gửi:
- Văn phòng Thành uỷ;
- Văn phòng Đoàn ĐBQH và HĐND TP Hà Nội;
- Văn phòng Uỷ ban MTTQ Việt Nam - TP Hà Nội;
- Văn phòng UBND Thành phố;
- Các Sở, ban, ngành, cơ quan ngang Sở;
- UBND các xã, phường.

Thực hiện công tác chuyên trách về bảo đảm an ninh mạng, an ninh thông tin mạng trên địa bàn Thành phố, qua công tác nắm tình hình trên không gian mạng, Công an thành phố Hà Nội phát hiện một số lỗ hổng bảo mật nghiêm trọng, nguy cơ gây mất an ninh mạng, an ninh thông tin mạng, cụ thể như sau:

1. Thông tin về các lỗ hổng bảo mật nghiêm trọng

(1) Lỗ hổng bảo mật trên thiết bị tường lửa Palo Alto Networks (CVE-2026-0300, điểm CVSS 9.3): Lỗ hổng bảo mật liên quan đến lỗi tràn bộ đệm trong tính năng xác thực người dùng *(User-ID Authentication Portal)*. Tin tặc không cần tài khoản hay tương tác của người dùng vẫn có thể thực thi mã tùy ý với đặc quyền root, từ đó theo dõi, truy cập mạng nội bộ và thu thập thông tin làm bàn đạp tấn công hệ thống.

(2) Lỗ hổng bảo mật trong trình duyệt Google Chrome (CVE-2026-5281, điểm CVSS 8.8): Lỗ hổng bảo mật phát sinh từ Lỗi "sử dụng sau khi giải phóng" *(use-after-free)* trong thành phần Dawn *(Dawn là một dự án mã nguồn mở trong hệ sinh thái Chromium, đóng vai trò bản thực thi tiêu chuẩn WebGPU – lớp trung gian quan trọng cho phép các ứng dụng web khai thác trực tiếp sức mạnh xử lý đồ họa của phần cứng máy tính)* của WebGPU. Tin tặc có thể lừa nạn nhân truy cập trang HTML độc hại để chiếm quyền kiểm soát tiến trình kết xuất, từ đó thực thi mã lệnh tùy ý, theo dõi hoạt động và đánh cắp dữ liệu.

(3) Lỗ hổng bảo mật trong Microsoft Defender (CVE-2026-33825, điểm CVSS 7.8): Lỗ hổng bảo mật tồn tại trên phần mềm diệt virus tích hợp trên Windows cho phép tin tặc tạo tệp tin giả mạo để lợi dụng quá trình rà quét của Defender. Qua đó, tin tặc có thể vô hiệu hóa lớp bảo vệ hệ thống, chiếm quyền điều khiển toàn bộ hệ thống *(System)* để cài mã độc, phần mềm gián điệp và đánh cắp thông tin.

(4) Chuỗi 15 lỗ hổng bảo mật trên Router Tenda F451 (điểm CVSS từ 9.0 đến 9.8): Dòng thiết bị này tồn tại 15 lỗ hổng bảo mật với điểm CVSS nghiêm trọng từ 9.0 đến 9.8 nằm trong các hàm cốt lõi như quản lý kết nối WAN, DHCP, định tuyến tĩnh. Kẻ tấn công có thể xâm nhập thiết bị tự động, chiếm quyền quản trị từ xa để đánh cắp toàn bộ thông tin nhạy cảm đi qua mạng và dùng thiết bị làm điểm "nằm vùng" tấn công vào máy chủ dữ liệu quan trọng.

2. Để tăng cường công tác bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ bí mật nhà nước, Công an Thành phố đề nghị các đơn vị triển khai các biện pháp khắc phục, cụ thể:

(1) Rà soát, cập nhật ngay các bản vá lỗi mới nhất cho toàn bộ phần mềm, trình duyệt và thiết bị tường lửa đang sử dụng, đồng thời thu hồi và loại bỏ hoàn toàn các thiết bị mạng hết vòng đời, ngừng sản xuất, không còn nhận được cập nhật phần mềm, bản vá bảo mật hoặc hỗ trợ kỹ thuật từ hãng.

(2) Phổ biến, quán triệt tới cán bộ, công chức, viên chức nâng cao ý thức cảnh giác, chấp hành nghiêm các quy định của pháp luật về bảo đảm an ninh mạng, an toàn thông tin và bảo vệ bí mật nhà nước.

Kết quả kiểm tra, rà soát, khắc phục đề nghị trao đổi bằng văn bản gửi về Công an thành phố Hà Nội ***trước ngày 22/5/2026*** (*qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, địa chỉ: 55 phố Lý Thường Kiệt, phường Cửa Nam, Hà Nội*). Công an thành phố Hà Nội cử đồng chí Nguyễn Hoàng Nam *(số điện thoại: 0978.224.789*) làm đầu mối liên hệ, phối hợp công tác.

Công an thành phố Hà Nội trao đổi để quý đơn vị phối hợp công tác./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc CATP (để báo cáo);
- Lưu: VT, ANM&PCTPSDCNC.Đ5.(N).05b.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ X.H.C.N VIỆT NAM
CÔNG AN THÀNH PHỐ HÀ NỘI

Đại tá Nguyễn Tiến Đạt