BỘ CÔNG AN
CÔNG AN TP HÀ NỘI

Số: 2590/CAHN-ANM&PCTPSDCNC
V/v cảnh báo các lỗ hổng bảo mật nghiêm trọng gây mất an ninh mạng, an toàn thông tin

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

Hà Nội, ngày 15 tháng 4 năm 2026

Kính gửi:

- Các Sở, ban, ngành, cơ quan ngang Sở;
- UBND các xã, phường thành phố Hà Nội.

Thực hiện chức năng, nhiệm vụ quản lý nhà nước về an toàn thông tin mạng trên địa bàn thành phố Hà Nội, Công an Thành phố phát hiện một số lỗ hổng bảo mật nghiêm trọng trên các nền tảng AI, máy chủ thiết bị mạng và ứng dụng phổ biến, tiềm ẩn nguy cơ gây mất an ninh mạng, an toàn thông tin, cụ thể như sau:

1. Nguy cơ xâm nhập từ nền tảng AI OpenClaw

Nền tảng AI OpenClaw *(ứng dụng AI tự vận hành – AI Agent)* có chức năng tự động rà soát, đọc tệp tin, khởi chạy ứng dụng trên thiết bị máy tính và thực hiện theo các yêu cầu của người dùng. Việc khai thác lỗ hổng bảo mật nghiêm trọng CVE-2026-33576 *(Mã định danh: CVE-2026-33576; Ngày công bố: 28/3/2026; Điểm CVSS: 9.8/10 – tương ứng với mức độ ảnh hưởng rất nghiêm trọng)* cho phép tin tặc chiếm quyền điều khiển, xâm nhập từ xa vào máy tính và ra lệnh cho AI Agent đánh cắp thông tin, dữ liệu, ảnh hưởng trực tiếp đến hoạt động của hệ thống thông tin.

2. Các lỗ hổng nghiêm trọng trên máy chủ, thiết bị mạng và trình duyệt web

- Các lỗ hổng bảo mật nghiêm trọng trên thiết bị định tuyến Router Tenda AC10 *(phiên bản firmware 16.03.10.10_multi_TDE01)*: Tồn tại các lỗ hổng bảo mật tràn bộ nhớ đệm, chèn lệnh hệ điều hành và sử dụng khóa mã hóa cứng *(CVE-2026-5550, CVE-2026-5548, CVE-2026-5547, CVE-2026-5549, được phát hiện đầu tháng 4/2026, điểm CVSS: 8.8/10)*. Khai thác lỗ hổng này, các đối tượng tấn công có thể thực thi mã từ xa với quyền cao nhất; chèn câu lệnh tại chức năng lọc địa chỉ MAC nhằm can thiệp sâu vào cấu hình hệ điều hành của thiết bị.

- Trên máy chủ và phần mềm quản trị Cisco *(Máy chủ Cisco UCS C-Series M5, M6, E-Series M3, M6; Catalyst 8300 Series Edge uCPE)*: Các lỗ hổng bảo mật *(CVE-2026-20093, CVE-2026-20094, CVE-2026-20095, CVE-2026-20096, CVE-2026-20160, được phát hiện đầu tháng 4/2026, điểm CVSS: 9.8/10)* cho phép tin tặc chiếm quyền quản trị cao nhất *(Admin)* trên bộ điều khiển máy chủ. Tin tặc có thể cài đặt mã độc vào firmware máy chủ ngay cả khi cài đặt lại hệ điều hành, cấu

hình BIOS. Đặc biệt, trình quản lý bản quyền phần mềm nội bộ của hãng này cho phép tin tặc có thể gửi các yêu cầu API độc hại nhằm thực thi các câu lệnh can thiệp trực tiếp vào hệ điều hành của máy chủ.

- Trên trình duyệt Google Chrome: Tồn tại các lỗ hổng bảo mật *(CVE-2026-5287, CVE-2026-5279, CVE-2026-5285, được phát hiện từ đầu tháng 4/2026, điểm CVSS: 8.8/10)* lợi dụng trình xem PDF tích hợp, tin tặc có thể tấn công phát tán tệp tin giả mạo qua thư điện tử hoặc mạng internet nhằm lừa nạn nhân thao tác mở tệp, từ đó chiếm đoạt quyền điều khiển, đánh cắp dữ liệu nhạy cảm. Đồng thời, công cụ JavaScript cho phép tin tặc thực thi các mã lệnh tùy ý trong môi trường sandbox của trình duyệt.

3. Từ tình hình trên, nhằm tăng cường công tác bảo đảm an ninh mạng, an ninh thông tin trên địa bàn thành phố Hà Nội, kịp thời phòng ngừa, ngăn chặn, ứng phó với các nguy cơ mất an ninh mạng, Công an Thành phố đề nghị các đơn vị khẩn trương thực hiện:

(1) Rà soát và khắc phục ngay các lỗ hổng bảo mật:

- Đối với nền tảng AI OpenClaw: Thực hiện rà soát trên các máy tính do đơn vị quản lý có cài đặt, sử dụng nền tảng ứng dụng OpenClaw, tiến hành cập nhật lên *phiên bản 2026.3.28* hoặc cao hơn. Đồng thời thiết lập các phân quyền bảo mật (*chỉ cho phép đọc/ghi không cho phép chạy file);* vô hiệu hóa chức năng tự động tải xuống để kiểm soát dữ liệu nguồn vào, giảm thiểu tối đa nguy cơ bị tấn công, khai thác. Tuyệt đối không cài đặt các AI Agent mã nguồn mở trên máy tính có kết nối mạng nội bộ của đơn vị khi chưa được cơ quan chức năng kiểm tra, đánh giá an ninh, an toàn.

- Đối với thiết bị Tenda AC10, hệ thống máy chủ và phần mềm quản trị Cisco: Tiến hành rà soát, kiểm tra phiên bản firmware của hệ thống thiết bị, phần mềm đang sử dụng; khẩn trương áp dụng biện pháp khắc phục các lỗ hổng bảo mật nghiêm trọng, cập nhật, nâng cấp Firmware/Software mới nhất *"AC10 V6.0 Firmware_V16.03.62.09";* sử dụng các công cụ giám sát để quét các bản ghi (logs) liên quan đến chuỗi ký tự HTTP bất thường; vô hiệu hóa tính năng quản lý thiết bị từ xa qua mạng Internet *(Remote Management).*

- Cập nhật trình duyệt Google Chrome lên phiên bản 146.0.7680.178. Trong trường hợp chưa có bản vá, cần xem xét tạm ngừng sử dụng hoặc áp dụng biện pháp cách ly mạng đối với các thiết bị này.

(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. Tuyệt đối không cung cấp, tải lên *(upload)* các tài liệu nội bộ, bí mật nhà nước hoặc đồng bộ hóa dữ liệu,

thông tin của cơ quan, đơn vị với các công cụ trí tuệ nhân tạo *(AI)* để tránh nguy cơ lộ, mất bí mật nhà nước hoặc khai thác thông tin, tài liệu nội bộ.

Kết quả rà soát, khắc phục yêu cầu các đơn vị tổng hợp, báo cáo bằng văn bản gửi về Công an thành phố Hà Nội **trước ngày** 24 **/4/2026** *(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 Trần Công Hoàng *(số điện thoại: 0776.827.888)* làm đầu mối đôn đốc, phối hợp.

Công an thành phố Hà Nội trao đổi các Quý cơ quan, đơn vị để phối hợp công tác./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc CATP (để báo cáo);
- Lưu: VT, ANM&PCTPSDCNC(Đ5).CH.04b.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Nguyễn Tiến Đạt