BỘ CÔNG AN
CÔNG AN TỈNH ĐỒNG THÁP

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

Số: 1305/CAT-ANM

V/v cảnh báo một số lỗ hổng bảo mật nghiêm trọng tháng 02/2026

Đồng Tháp, ngày 10 tháng 3 năm 2026

Kính gửi:
- Các sở, ban, ngành, đơn vị sự nghiệp, doanh nghiệp nhà nước thuộc tỉnh;
- Ủy ban nhân dân các xã, phường.

Thời gian qua, nhiều lỗ hổng, nguy cơ bảo mật được phát hiện, công bố có khả năng bị các tin tặc khai thác, tấn công vào hệ thống thông tin cơ quan, tổ chức nhà nước, doanh nghiệp, cụ thể:

- Lỗ hổng CVE-2026-21519 trong Desktop Window Manager, cho phép đối tượng tấn công leo thang đặc quyền và kiểm soát hoàn toàn hệ thống;

- Lỗ hổng CVE-2026-22719 trong VMware Aria Operations, cho phép đối tượng tấn công từ xa, không cần xác thực, chèn lệnh độc hại và thực thi trên hệ thống bị ảnh hưởng.

- Lỗ hổng CVE-2026-21509 trong Microsoft Office, cho phép đối tượng tấn công vượt qua các cơ chế bảo vệ cục bộ của Office, từ đó thực hiện các hành vi tấn công tiếp theo sâu vào hệ thống.

- Lỗ hổng CVE-2025-11953 trong React Native CLI, cho phép đối tượng tấn công thực thi mã tùy ý từ xa vào hệ thống bị ảnh hưởng.

- Lỗ hổng CVE-2026-1592 trong Foxit PDF Editor Cloud, cho phép đối tượng tấn công thực thi mã JavaScript tùy ý trong ngữ cảnh của người dùng.

- Phần mềm gián điệp mới ZeroDayRAT cho phép kẻ tấn công có thể nhắm mục tiêu vào người dùng iPhone và Android.

- Mã độc Anatsa được phát hiện trong ứng dụng trên điện thoại Android "All Document Reader" cho phép kẻ tấn công chiếm quyền các ứng dụng ngân hàng, tài liệu trong điện thoại của người dùng.

Tình hình trên, để bảo đảm an toàn hệ thống thông tin trên địa bàn tỉnh, Công an tỉnh đề nghị quý cơ quan, đơn vị chủ động rà soát trên hệ thống thông tin do cơ quan, đơn vị mình quản lý, vận hành để phòng ngừa, kịp thời cập nhật bản vá. Khi phát sinh tình hình có liên quan, kịp thời trao đổi về Công an tỉnh (qua Phòng an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại

0693.599.332) để phối hợp xử lý *(gửi kèm phụ lục chi tiết các lỗ hổng và các biện pháp phòng ngừa)./.*

Nơi nhận:
- Như kính gửi;
- Đ/c Giám đốc CAT (để báo cáo);
- Phòng ANM&PCTPSDCNC (để thực hiện);
- Lưu CAT: VT, ANM(Đ4).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Nguyễn Minh Tân

PHỤ LỤC

(Kèm theo Công văn số /CAT-ANM, ngày /3/2026 của Công an tỉnh)

1. CVE-2026-21519 trong Desktop Window Manager

a) Mô tả

- Điểm CVSS: 7.8/10; Mức độ: Cao;

- Lỗ hổng CWE-843 xảy ra khi DWM xử lý tài nguyên đồ họa không kiểm tra đúng kiểu dữ liệu, dẫn đến nhầm lẫn kiểu trong quá trình tổng hợp giao diện người dùng. Kẻ tấn công khai thác bằng cách tạo dữ liệu đầu vào độc hại gây hỏng bộ nhớ heap và thực thi mã tùy ý, đã bị khai thác zero-day trong thực tế.

b) Phiên bản ảnh hưởng: Ảnh hưởng chủ yếu đến Windows 10 phiên bản 1607.

c) Khuyến nghị: Cập nhật ngay các bản vá từ Microsoft qua Windows Update.

2. CVE-2026-22719 trong VMware Aria Operations

a) Mô tả

- Điểm CVSS: 8.1/10; Mức độ: Cao;

- Lỗ hổng CWE-77 xảy ra do thiếu kiểm tra dữ liệu đầu vào của người dùng trong support-assisted migration workflow, nơi dữ liệu đầu vào được chèn trực tiếp vào system command mà không kiểm tra ký tự đặc biệt (; | & `). Kẻ tấn công network-accessible có thể chèn lệnh tùy ý chạy với quyền Aria Operations service.

b) Phiên bản ảnh hưởng:

- VMware Aria Operations 8.x (đã vá ở 8.18.6).

- VMware Cloud Foundation 9.x.x.x (đã vá ở 9.0.2.0).

- VMware vSphere Foundation 9.x.x.x (đã vá ở 9.0.2.0).

c) Khuyến nghị: Cập nhật ngay các bản vá.

3. CVE-2026-21509 trong Microsoft Office

a) Mô tả

- Điểm CVSS: 7.8/10; Mức độ: Cao;

- Lỗ hổng (CWE-807) xảy ra khi Office xử lý RTF hoặc tài liệu nhúng OLE không kiểm tra đúng "kill bit" cho COM objects, vượt qua các biện pháp bảo vệ tích hợp. Kẻ tấn công dùng phishing gửi file Word/Excel độc hại nhúng CLSID {EAB22AC3-30C1-11CF-A7EB-0000C05BAE0B}, tải payload từ WebDAV hoặc remote server, đã bị APT28 khai thác zero-day.

b) Phiên bản ảnh hưởng:

- Microsoft Office 2016 (32/64-bit), 2019.

- Office LTSC 2021, LTSC 2024.

- Microsoft 365 Apps for Enterprise (trước vá 26/1/2026).

c) Khuyến nghị: Cập nhật ngay các bản vá từ Microsoft qua Windows Update.

4. CVE-2025-11953 trong React Native CLI

a) Mô tả

- Điểm CVSS: 9.8/10; Mức độ: Rất Cao;

- Server Metro mặc định bind 0.0.0.0 (lắng nghe tất cả interface), expose endpoint như /symbolicate hoặc /open-url chấp nhận dữ liệu đầu vào người dùng mà không kiểm tra, truyền trực tiếp vào hàm open() hoặc system shell dẫn đến RCE. Kẻ tấn công gửi POST request độc hại (ví dụ inject "&& whoami" vào logPath) để chạy lệnh như calc.exe; đã bị khai thác thực tế từ 21/12/2025.

b) Phiên bản ảnh hưởng:

- @react-native-community/cli-server-api 4.8.0 đến 20.0.0-alpha.2 (vá từ 20.0.0).

- React Native ≤ 0.74.1, Metro ≤ 0.81.0.

- Tất cả nền tảng (Windows nghiêm trọng nhất), dự án dùng npx react-native start hoặc npm start.

c) Khuyến nghị: Nâng cấp ngay @react-native-community/cli lên ≥20.0.0 và Metro ≥0.82.0; cấu hình server chỉ bind localhost (--host 127.0.0.1). Kiểm tra bằng "npm list @react-native-community/cli-server-api".

5. CVE-2026-1592 trong Foxit PDF Editor Cloud

a) Mô tả

- Điểm CVSS: 6.4/10; Mức độ: Trung bình;

- Lỗ hổng CWE-79 xảy ra khi ứng dụng không kiểm tra dữ liệu đầu vào của người dùng trong trường tên/mô tả layer, nhúng trực tiếp vào HTML output. Mã độc lưu trữ trên server và thực thi trong trình duyệt nạn nhân khi họ xem layer bị nhiễm, có thể đánh cắp session cookie hoặc thực hiện hành động thay nạn nhân.

b) Phiên bản ảnh hưởng: Foxit PDF Editor Cloud (pdfonline.foxit.com) tất cả phiên bản trước ngày 2026-02-03.

c) Khuyến nghị: Cập nhật ngay lên phiên bản Foxit PDF Editor Cloud từ 2026-02-03 trở lên; kiểm tra và xóa layer đáng ngờ. Áp dụng CSP header nghiêm ngặt, hạn chế quyền tạo layer cho người dùng tin cậy, triển khai WAF chặn XSS payload.

6. Phần mềm gián điệp mới ZeroDayRAT

a) ZeroDayRAT là phần mềm gián điệp thương mại mới (xuất hiện đầu 2026) được bán trên Telegram, cho phép đối tượng tấn công kiểm soát hoàn toàn iPhone (iOS lên đến 26) và Android (5-16) qua dashboard web trực quan.

b) Khả năng tấn công

- Theo dõi GPS thời gian thực, xem vị trí trên Google Maps.

- Truy cập camera trước/sau, micro để do thám trực tiếp.

- Đọc SMS, thông báo, OTP để bypass 2FA; keylogging app usage.

- Ăn cắp crypto từ Coinbase, Binance, MetaMask; overlay giả mạo banking apps (Apple Pay, Google Pay).

c) Phương thức lây nhiễm

Phổ biến qua smishing (SMS lừa cài APK Android hoặc payload iOS), phishing email, fake apps trên chợ ứng dụng giả mạo, link độc hại qua WhatsApp/Telegram.

d) Khuyến nghị: Không cài app từ SMS/link lạ; chỉ dùng Google Play/App Store chính thức. Bật xác thực 2FA app-based thay SMS; cập nhật iOS/Android mới nhất. Dùng phần mềm phòng chống mã độc như Malwarebytes/Kaspersky; kiểm tra ứng dụng lạ, kiểm tra việc cấp quyền camera/micro. Giám sát tài khoản ngân hàng/crypto bất thường; xóa ứng dụng đáng ngờ.

7. Mã độc Anatsa được phát hiện trong ứng dụng trên điện thoại Android "All Document Reader"

a) Được phát hiện trong ứng dụng Android giả mạo "All Document Reader" (hoặc tương tự "Document Reader – File Manager") trên Google Play Store, đã lây nhiễm hơn 50.000 thiết bị trước khi bị gỡ bỏ.

b) Khuyến nghị: Kiểm tra và gỡ ngay "All Document Reader" hoặc app document lạ; quét bằng Malwarebytes/Kaspersky/Zscaler. Bật Google Play Protect, tránh cấp quyền cho ứng dụng không tin cậy; cập nhật Android mới nhất.