SỞ Y TẾ TỈNH ĐỒNG THÁP
TRUNG TÂM Y TẾ
KHU VỰC TÂN PHƯỚC

Số: 392 /TTYTTP-TCHC
V/v cảnh báo một số lỗ hổng bảo mật tháng 02 năm 2026

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

Tân Phước 1, ngày 19 tháng 3 năm 2026

Kính gửi: Khoa, phòng thuộc Trung tâm Y tế.

Thực hiên theo tinh thần Công văn số 1817/SYT-VP ngày 13/3/2026 của Sở Y tế tỉnh Đồng Tháp về việc cảnh báo một số lỗ hổng bảo mật tháng 02 năm 2026;

Trước tình hình an toàn thông tin diễn biến phức tạp với nhiều lỗ hổng nghiêm trọng có nguy cơ bị tin tặc khai thác, tấn công vào hệ thống thông tin của các cơ quan nhà nước. Nhằm đảm bảo an toàn cho hệ thống thông tin của đơn vị, Ban Giám đốc Trung tâm Y tế đề nghị lãnh đạo Khoa, phòng khẩn trương triển khai thực hiện các nội dung sau:

1. Thường xuyên kiểm tra máy tính cá nhân, máy tính bàn đang sử dụng tại đơn vị có khả năng bị ảnh hưởng, thực hiện cập nhật bản vá kịp thời để tránh nguy cơ bị tấn công mạng vào các lỗ hỏng.

2. Đề nghị viên chức và người lao động tại đơn vị tăng cường giám sát và thực hiện phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng. Đồng thời theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Thông tin đến viên chức một số lỗ hổng bảo mật nghiêm trọng tháng 02/2026:

3.1. 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.

3.2. 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 Wrord/Excel độc hại nhúng CLSID {EAB22AC3-30C1-11CF-A7EB-0000C05BAEOB}, tài 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.

3.3. 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.

Khi Khoa phòng phát sinh tình hình có liên quan, kịp thời báo cáo về Phòng Tổ chức Hành chính *(qua Tổ Công nghệ thông tin)* để được hướng dẫn thực hiện. Phòng Tổ chức Hành chính báo cáo 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*) Sở Y tế để xin ý kiến phối hợp xử lý./.

Nơi nhận:
- Như trên (t/h);
- Ban Giám đốc TTYT (b/c);
- Trang thông tin điện tử TTYT;
- Lưu: VT, TCHC.

GIÁM ĐỐC

SỞ Y TẾ TỈNH ĐỒNG THÁP
TRUNG TÂM Y TẾ KHU VỰC TÂN PHƯỚC

Trần Thanh Hải