BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

Số: 1614 /CAT-ANM

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

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

Quảng Ngãi, ngày 23 tháng 3 năm 2026

Kính gửi:
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Văn phòng Tỉnh ủy, UBND tỉnh;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Các sở, ban ngành và hội đoàn thể tỉnh;
- Bộ Chỉ huy Quân sự tỉnh; Tòa án nhân dân tỉnh;
- Viện Kiểm sát nhân dân tỉnh; Thi hành án dân sự tỉnh;
- Bảo hiểm xã hội tỉnh; Cảng vụ Hàng hải Quảng Ngãi;
- Thống kê tỉnh; Thuế tỉnh Quảng Ngãi;
- Kho bạc Nhà nước khu vực XV;
- Báo và Phát thanh, Truyền hình Quảng Ngãi;
- Các Trường: Đại học Phạm Văn Đồng, Cao đẳng Kon Tum, Cao đẳng Việt Nam - Hàn Quốc - Quảng Ngãi;
- Công ty CP Lọc hóa dầu Bình Sơn; Truyền tải điện Quảng Ngãi; Điện lực Quảng Ngãi;
- UBND các xã, phường, Đặc khu Lý Sơn.

Trong tháng 02/2026, qua công tác bảo đảm an toàn thông tin an ninh ninh mạng, lực lượng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Công an tỉnh đã thực hiện phân tích và tổng hợp đối với 10 lỗ hổng bảo mật nghiêm trọng ảnh hưởng đến hệ thống thông tin trên địa bàn tỉnh *(Tài liệu lưu hành nội bộ)*. Trong đó, có 04 lỗ hổng bảo mật mức độ nghiêm trọng rất cao, 06 lỗ hổng bảo mật mức độ nghiêm trọng cao, cụ thể:

1. Lỗ hổng bảo mật trên hệ điều hành và các ứng dụng của Microsoft

1.1. Lỗ hổng CVE-2026-21259 nâng quyền cục bộ (Local Privilege Escalation) trên Microsoft Office Excel

- Đánh giá mức độ nghiêm trọng: Cao (Điểm CVSS: 7.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng xuất phát từ lỗi quản lý bộ nhớ dạng "heap-based buffer overflow khi Excel xử lý dữ liệu. Khi dữ liệu vượt quá vùng nhớ được cấp phát, cấu trúc bộ nhớ bị ghi đè, tạo điều kiện cho tin tặc chèn và thực thi mã tùy ý.

+ Đối tượng gửi tệp Excel độc hại bị thay đổi cấu trúc bên trong (ví dụ: thay đổi giá trị độ dài trong thành phần XML của định dạng .xlsx hoặc record dữ liệu trong .xls) đến người dùng (qua email, thiết bị ngoại vi...). Khi người dùng mở tệp,

Excel tiến hành phân tích cú pháp (parse) các thành phần dữ liệu, do giá trị độ dài sai lệch và Excel cấp phát bộ nhớ heap không đủ, quá trình xử lý dữ liệu sẽ ghi vượt giới hạn bộ đệm, làm ghi đè cấu trúc điều khiển bộ nhớ và cho phép chuyển hướng luồng thực thi đến mã độc được nhúng sẵn (Shellcode). Sau khi chiếm quyền thực thi, shellcode tải thêm payload từ máy chủ điều khiển và chạy với quyền của người dùng hiện tại, từ đó tin tặc có thể cài backdoor, thu thập thông tin hoặc khai thác leo thang đặc quyền trên hệ thống.

- Phiên bản ảnh hưởng: Microsoft 365 Apps, Microsoft Office 2019, Office LTSC.

- Hướng xử lý, khắc phục: Cập nhật bản vá *(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21259);* bật Protected View cho tài liệu tải từ internet và triển khai cơ chế kiểm soát ứng dụng (Applocker/WDAC).

1.2. Lỗ hổng CVE-2026-21514 vượt qua cơ chế bảo mật (Security Feature Bypass) trên Microsoft Office Word

- Đánh giá mức độ nghiêm trọng: Cao (Điểm CVSS: 7.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh do Microsoft Office Word dựa vào dữ liệu đầu vào chưa được xác thực đầy đủ trong các quyết định bảo mật liên quan đến cơ chế OLE *(Object linking and Embedding)* dẫn đến bỏ qua cảnh báo bảo mật.

+ Tin tặc gửi đến người dùng tệp tin Word có chứa đối tượng OLE độc hại, khi người dùng mở tài liệu, cơ chế cảnh báo bị vượt qua và thành phần nhúng có thể tải hoặc thực thi mã độc mà không bị ngăn chặn trên hệ thống.

- Phiên bản ảnh hưởng: Microsoft 365 Apps, Office LTSC (2021, 2024).

- Hướng xử lý, khắc phục: Cập nhật bản vá *(đường link bản vá: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21514)*. Hạn chế hoặc vô hiệu hóa OLE nếu không cần thiết và tăng cường giám sát hành vi bất thường như word tự khởi tạo Powershell.

1.3. Lỗ hổng leo thang đặc quyền CVE-2026-21533 tồn tại trong thành phần Windows Remote Desktop Services của hệ điều hành Microsoft Windows:

- Đánh giá mức độ nghiêm trọng: Cao (Điểm CVSS: 7.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng xuất phát từ cơ chế quản lý và kiểm soát đặc quyền chưa đầy đủ trong dịch vụ RDS, cho phép người dùng quyền thấp có thể thực hiện thao tác dẫn tới leo thang đặc quyền lên mức SYSTEM.

+ Kẻ tấn công sở hữu và đăng nhập vào một tài khoản thông thường quyền

thấp (qua câu nhử phising; dò quét tài khoản mật khẩu; đánh cắp tài khoản...), từ tài khoản này, kẻ tấn công chạy một chương trình gửi yêu cầu tới dịch vụ chứa lỗ hổng, kèm theo tham số trỏ đến một đường dẫn hoặc khóa registry do họ kiểm soát, do thiếu kiểm tra quyền, dịch vụ đang chạy với quyền SYSTEM sẽ thực hiện thao tác thay cho người dùng (ví dụ như ghi đè một tệp thực thi trong thư mục hệ thống, tạo hoặc sửa khóa registry autorun ở mức "machine"), từ đó ở lần khởi động tiếp theo (hoặc khi dịch vụ được gọi lại), mã do kẻ tấn công đặt vào sẽ được chạy với quyền SYSTEM, hoàn tất việc leo thang đặc quyền.

- Phiên bản ảnh hưởng: Windows 10, 11 và Windows Server từ 2012 đến 2025.

- Hướng xử lý, khắc phục: Cài đặt bản vá từ nhà sản xuất Microsoft (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21533); hạn chế quyền local administrator và vô hiệu hóa hoặc giới hạn RDP khi không cần thiết.

1.4. Lỗ hổng vượt qua cơ chế bảo mật (Security Feature Bypass) CVE-2026-21510 trong Windows Shell

- Đánh giá mức độ nghiêm trọng: Cao (Điểm CVSS: 8.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng này bắt nguồn từ lỗi xử lí logic trong thành phần windows shell của hệ điều hành windows, cụ thể là cơ chế kiểm tra và thực thi chính sách bảo mật đối với tệp Shortcut tải từ internet, cho phép kẻ tấn công vượt qua các cơ chế bảo vệ như Window SmartScreen và các cảnh báo về nguồn gốc tệp trước khi thực thi nội dung được tải về.

+ Trong trường hợp cụ thể, tin tặc có thể tạo một tệp shortcut (.lnk) hoặc tệp nén chứa shortcut được cấu hình đặc biệt nhằm làm sai lệch cơ chế đánh dấu bảo mật Mark-of-the-web (MOTW) và gửi cho người dùng (qua câu nhử phising, tán phát trên mạng). Khi người dùng tải về từ internet và nhấp mở tệp, do lỗi xử lý trong windows Shell, cơ chế kiểm tra nguồn gốc tệp không được kích hoạt đúng cách, khiến cảnh báo bảo mật không hiển thị, nội dung shortcut trỏ tới (ví dụ tệp thực thi hoặc script) sẽ chạy ngay với quyền người dùng hiện tại, mở đường cho việc tải và thực thi mã độc tiếp theo.

- Phiên bản ảnh hưởng: Các phiên bản Window 10 (1607, 1809, 21H2, 22H2), Window 11 (23H2, 24H2, 25H2 và 26H1), Window Server 2012, 2016, 2019, 2022, 2025 *(các build trước bản vá tháng 2/2026)*.

- Hướng xử lý khắc phục: Cập nhật bản vá từ link nhà cung cấp (https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21510). Không tải về hoặc nhấp vào các liên kết hoặc tệp shortcut không rõ nguồn gốc.

2. Lỗ hổng bảo mật tồn tại thiết bị hãng Fortinet (*CVE-2026-22153)*

- Đánh giá mức độ nghiêm trọng: Rất cao (Điểm CVSS: 9.1/10).

- Mô tả kỹ thuật:

+ Lỗ hổng này thuộc loại Authentication Bypass by Primary Weakness (CWE-305), xảy ra trong cơ chế xác thực đa yếu tố hoặc xác thực qua các máy chủ trung gian (như RADIUS/LDAP) trên FortiOS. Lỗi phát sinh do thuật toán xử lý logic xác thực không chặt chẽ. Kẻ tấn công có thể gửi các gói tin phản hồi xác thực được "chế" lại, khiến thiết bị tin rằng quá trình đăng nhập đã thành công mà không cần kiểm tra mật khẩu thực tế hoặc mã OTP.

+ Kẻ tấn công đánh lừa tiến trình authd của Fortinet bằng cách thao túng các tham số trong luồng xác thực (Authentication Flow), dẫn đến việc thiết bị cấp quyền truy cập ngay lập tức. Có thể cấp quyền quản trị (Super_Admin), cho phép thay đổi cấu hình, tạo người dùng mới hoặc kiểm soát toàn bộ lưu lượng mạng đi qua thiết bị.

- Phiên bản ảnh hưởng: Lỗ hổng tác động đến các dòng sản phẩm sử dụng cấu hình xác thực từ xa hoặc cổng VPN.

+ FortiOS: Phiên bản từ 7.2.0 đến 7.2.11; 7.4.0 đến 7.4.3.

+ FortiProxy: Phiên bản từ 7.2.x và 7.4.x.

+ FortiSwitchManager: Một số phiên bản chạy hệ điều hành cũ.

- Hướng xử lý khắc phục: Nâng cấp ngay lên FortiOS 7.6.5 hoặc mới hơn - bản vá đã được Fortinet phát hành. Nếu chưa thể nâng cấp, xem xét tạm thời vô hiệu hóa Agentless VPN hoặc FSSO policy sử dụng LDAP; giới hạn truy cập từ bên ngoài vào dịch vụ VPN; tăng cường giám sát log LDAP và FortiOS để phát hiện hành vi bất thường.

3. Lỗ hổng bảo mật tồn tại thiết bị hãng Dell *(CVE-2026-22769)*

- Đánh giá mức độ nghiêm trọng: Rất cao (Điểm CVSS: 9.8/10).

- Mô tả kỹ thuật:

+ Đây là một lỗ hổng Zero-day đã bị khai thác trong các chiến dịch tấn công nhắm mục tiêu vào cơ sở hạ tầng ảo hóa. Lỗ hổng này thuộc loại Command Injection (Chèn lệnh) nằm trong giao diện quản trị web của Dell RecoverPoint for VMs. Lỗi phát sinh do việc thiếu kiểm tra và làm sạch (sanitization) dữ liệu đầu vào trong các yêu cầu API cụ thể được gửi đến cụm điều khiển (vRPA).

+ Kẻ tấn công từ xa, không cần xác thực, có thể gửi một gói tin HTTP được chế tạo đặc biệt chứa các ký tự điều khiển hệ thống (như ;, &&, hoặc |) vào các tham số đầu vào. Khi thiết bị xử lý yêu cầu này, nó sẽ vô tình thực thi các lệnh hệ điều hành tùy ý với quyền hạn cao nhất (root). Điều này cho phép kẻ tấn công cài đặt cửa hậu (backdoor), đánh cắp dữ liệu sao lưu hoặc phá hoại toàn bộ hệ thống phục hồi thảm họa của doanh nghiệp.

- Phiên bản ảnh hưởng: Lỗ hổng tác động trực tiếp đến các phiên bản của giải pháp Dell RecoverPoint for Virtual Machines:

+ Tất cả các phiên bản 5.3.x (trước phiên bản 5.3.4).

+ Tất cả các phiên bản 5.4.x (trước phiên bản 5.4.1).

- Hướng xử lý khắc phục: Cập nhật ngay lập tức: Nâng cấp hệ thống lên các phiên bản đã được vá lỗi:

+ RecoverPoint for VMs phiên bản 5.3.4 (Bản vá ổn định cho nhánh 5.3).

+ RecoverPoint for VMs phiên bản 5.4.1 (Bản vá mới nhất).

4. Lỗ hổng bảo mật tồn tại thiết bị Apple *(CVE-2026-20700)*

- Đánh giá mức độ nghiêm trọng: Cao (Điểm CVSS 7.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng này là một lỗi Memory Corruption (Hư hỏng bộ nhớ) nằm trong thành phần dyld (Dynamic Link Editor) của Apple; phát sinh do việc quản lý trạng thái (state management) không đúng cách trong quá trình dyld nạp và liên kết các thư viện động (dynamic libraries) vào bộ nhớ.

+ Kẻ tấn công có khả năng ghi vào bộ nhớ (memory write capability) có thể lợi dụng sơ hở này để thực thi mã tùy ý (Arbitrary Code Execution).

- Phiên bản ảnh hưởng: Lỗ hổng này tác động diện rộng đến hầu hết các hệ điều hành hiện tại của Apple:

+ iOS và iPadOS: Các phiên bản trước 26.3 và 18.7.5.

+ macOS Tahoe: Các phiên bản trước 26.3.

+ macOS Sequoia: Các phiên bản trước 15.7.4.

+ macOS Sonoma: Các phiên bản trước 14.8.4.

+ tvOS, watchOS và visionOS: Các phiên bản trước 26.3.

- Hướng xử lý khắc phục: Cập nhật hệ điều hành:

+ Nâng cấp lên iOS 26.3 / iPadOS 26.3 (hoặc bản cũ hơn là 18.7.5 cho các thiết bị đời cũ).

+ Nâng cấp lên macOS Tahoe 26.3, macOS Sequoia 15.7.4, hoặc macOS Sonoma 14.8.4.

+ Cập nhật watchOS 26.3, tvOS 26.3 và visionOS 26.3.

5. Lỗ hổng bảo mật tồn tại nền tảng WordPress *(CVE-2026-1357)*

- Đánh giá mức độ nghiêm trọng: Rất cao (Điểm CVSS: 9.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng này không nằm trong nhân (core) của WordPress mà xuất phát từ một lỗi logic trong việc xử lý tệp tin của các plugin phổ biến (đặc biệt là các plugin hỗ trợ tải lên và xử lý tệp tin đa phương tiện). Lỗ hổng phát sinh do việc thiếu kiểm tra (validation) và làm sạch (sanitization) dữ liệu đầu vào khi xử lý các yêu cầu tải tệp lên qua API hoặc giao diện web.

+ Kẻ tấn công gửi các yêu cầu HTTP chứa mã PHP độc hại được ngụy trang dưới dạng tệp tin hợp lệ. Do cơ chế kiểm tra phần mở rộng tệp tin (file extension)

hoặc loại tệp (MIME type) bị bỏ qua hoặc thực hiện sai cách, mã độc sẽ được lưu trữ và thực thi trên máy chủ. Kẻ tấn công có thể chạy các lệnh hệ thống, truy cập cơ sở dữ liệu, thay đổi nội dung trang web hoặc cài đặt các cửa hậu (backdoor) để duy trì quyền truy cập lâu dài.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng đến một loạt các plugin quản lý File Manager, Image Optimizer, và các thành phần Upload tích hợp trong các Theme tùy biến. Các phiên bản plugin được phát hành trước tháng 01/2026.

- Hướng xử lý khắc phục: Cập nhật tất cả lên phiên bản mới nhất có sẵn trong kho ứng dụng WordPress. Xóa các plugin không cần thiết, đặc biệt là các plugin quản lý tệp tin (File Managers) thường xuyên bị khai thác. Sử dụng các công cụ bảo mật để quét toàn bộ mã nguồn website nhằm phát hiện các tệp tin lạ hoặc mã độc đã được chèn vào trước đó.

6. Lỗ hổng bảo mật tồn tại thiết bị hãng Cisco *(CVE-2026-20127)*

- Đánh giá mức độ nghiêm trọng: Rất cao (Điểm CVSS: 10/10).

- Mô tả kỹ thuật:

+ Lỗ hổng qua mặt xác thực (Authentication Bypass) này bắt nguồn từ lỗi trong cơ chế xác thực kết nối ngang hàng (peering authentication) thuộc quy trình control-plane của hạ tầng mạng. Xảy ra trên hai thành phần cốt lõi của kiến trúc là Cisco Catalyst SD-WAN Controller (trước đây là vSmart) và Cisco Catalyst SD-WAN Manager (trước đây là vManage).

+ Kẻ tấn công từ xa, hoàn toàn không cần thông tin xác thực, có thể gửi các luồng yêu cầu mạng (crafted requests) được tinh chỉnh đặc biệt đến hệ thống mục tiêu. Hệ thống bị đánh lừa và cấp cho kẻ tấn công quyền truy cập dưới danh nghĩa một tài khoản nội bộ có đặc quyền cao (high-privileged, non-root user). Sau khi có quyền kiểm soát, tin tặc sẽ lạm dụng giao thức NETCONF (thường qua cổng TCP/830) và SSH để kết nối giữa các thiết bị quản trị, từ đó sửa đổi cấu hình mạng, chỉnh sửa template/policy của toàn bộ mạng lưới SD-WAN. Thực tế còn ghi nhận kẻ tấn công tiến hành xóa log trong /var/log để xóa dấu vết và cố tình hạ cấp (downgrade) phiên bản phần mềm hệ thống để leo thang đặc quyền lên mức root.

- Phiên bản ảnh hưởng: Các phiên bản phần mềm bị ảnh hưởng cụ thể:

+ Các phiên bản Cisco Catalyst SD-WAN cũ hơn 20.9.1.

+ Các thiết bị bị phơi bày giao diện quản lý ra ngoài Internet có rủi ro bị nhắm mục tiêu cao nhất.

- Hướng xử lý khắc phục: Cập nhật ngay lập tức hệ thống SD-WAN lên các phiên bản phần mềm đã được vá lỗi (Ví dụ: Chuyển lên các bản release an toàn thuộc nhánh 20.9.8.2 hoặc 20.12.6.1 tùy theo lộ trình cập nhật của doanh nghiệp). Ngắt các quyền truy cập quản trị mạng từ các mạng không an toàn (Internet). Chỉ cho phép các host đáng tin cậy truy cập vào Controller/Manager thông qua tường lửa. Vô hiệu hóa HTTP cho cổng web UI của SD-WAN Manager.

7. Lỗ hổng bảo mật tồn tại trong thư viện jsPDF *(CVE-2026-25755)*

- Đánh giá mức độ nghiêm trọng: Cao (Điểm CVSS: 8.8/10).

- Mô tả kỹ thuật:

+ Thư viện jsPDF là một thư viện phổ biến giúp tạo các tệp PDF bằng JavaScript. Lỗ hổng này xảy ra ở phương thức addJS (được sử dụng để chèn mã JavaScript vào PDF). Nếu dữ liệu đầu vào của người dùng không được làm sạch (sanitize) trước khi truyền vào phương thức addJS, kẻ tấn công có thể chèn các đối tượng PDF tùy ý (PDF Object Injection) vào tài liệu được tạo. Bằng cách thiết kế một payload đặc biệt có khả năng thoát (escape) khỏi dấu phân cách chuỗi của JavaScript, kẻ tấn công có thể chèn các mã độc hại vào tệp PDF. Khi có người dùng mở tệp PDF bị nhiễm độc này, tính năng tự động thực thi mã script (thường gặp qua AcroJS) sẽ được kích hoạt, dẫn đến việc kẻ tấn công có thể qua mặt cơ chế an toàn (sandbox bypass), làm thay đổi cấu trúc tài liệu hoặc thực thi các hành động độc hại khác trên máy nạn nhân.

+ Lỗ hổng này có thể bị khai thác từ xa (Remotely Exploitable) và đã có các mã khai thác (Proof of Concept - PoC) được công bố công khai.

- Phiên bản ảnh hưởng: Các phiên bản jsPDF trước 4.2.0 (jspdf < 4.2.0).

- Hướng xử lý khắc phục:

+ Nâng cấp thư viện jsPDF lên phiên bản 4.2.0 hoặc mới hơn.

+ Biện pháp thay thế (Workaround) trong trường hợp chưa thể cập nhật: Phải thực hiện quá trình "escape" (thoát/xử lý) toàn bộ các dấu ngoặc đơn () trong các đoạn mã JavaScript do người dùng cung cấp trước khi truyền chúng vào phương thức addJS. Việc này sẽ ngăn chặn mã độc thoát ra khỏi chuỗi và bị coi là một phần thực thi của cấu trúc PDF.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin góp phần bảo đảm an toàn các cơ quan, đơn vị trên địa bàn tỉnh, Công an tỉnh đề nghị lãnh đạo các đơn vị tiếp tục chỉ đạo rà soát, kiểm tra các dịch vụ, phần mềm đang sử dụng, kịp thời cập nhật, vá lỗi hệ thống nếu phát hiện tồn tại các lỗ hổng trên, tăng cường triển khai các biện pháp giám sát liên tục các hệ thống thông tin, phát hiện sớm các dấu hiệu bất thường, tấn công mạng. Trong quá trình thực hiện nếu có khó khăn, vướng mắc kịp thời liên hệ Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại 088.830.9485)* để được hỗ trợ.

Đề nghị các đồng chí quan tâm chỉ đạo thực hiện./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Phòng Tham mưu;
- Lưu: VT, ANM.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
CÔNG AN TỈNH QUẢNG NGÃI

Thiếu tướng Hồ Song Ân