BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

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

Số: 2162 /CAT-ANM

V/v cảnh báo lỗ hổng bảo mật nghiêm trọng tháng 3/2026

Quảng Ngãi, ngày 10 tháng 4 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 3/2026, qua công tác bảo đảm an toàn thông tin, an 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 12 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 03 lỗ hổng bảo mật mức độ nghiêm trọng rất cao, 09 lỗ hổng bảo mật mức độ nghiêm trọng cao, cụ thể:

1. Lỗ hổng bảo mật trên Microsoft SQL Server

1.1. Lỗ hổng CVE-2026-26115 leo thang đặc quyền (Elevation of Privilege - EoP) trong hệ quản trị cơ sở dữ liệu Microsoft SQL Server

- Đánh giá mức độ nghiêm trọng: Cao, điểm CVSS: 8.8/10.

- Mô tả kỹ thuật:

+ Lỗ hổng xuất phát từ việc kiểm tra không đúng kiểu dữ liệu đầu vào (improper Validation of Specified of input - CWE-1287). Do hệ thống phát sinh lỗi không xác thực chặt chẽ kiểu dữ liệu do người dùng cung cấp, dẫn đến tình trạng xử lý sai kiểu dữ liệu của một đối tượng trong bộ nhớ (type confusion - CWE-843) hoặc ép kiểu sai, từ đó cho phép vượt qua cơ chế kiểm soát truy cập và thực thi hành vi với quyền cao hơn.

+ Tình huống khai thác: Đối tượng thông qua tài khoản hợp lệ với quyền thấp trong hệ thống SQL Server (ví dụ như tài khoản user ứng dụng). Thông qua việc gửi các truy vấn hoặc payload đặc biệt (malformed input), đối tượng tiến hành khai thác lỗi kiểm tra kiểu dữ liệu để đánh lừa hệ thống, từ đó thực hiện các thao tác yêu cầu quyền cao như thay đổi role, truy cập dữ liệu nhạy cảm hoặc thậm chí chiếm quyền quản trị database.

- Phiên bản ảnh hưởng: Các phiên bản SQL Server 2016, 2017, 2019, 2022, 2025 *(chưa được cập nhật, cài đặt bản vá)*.

- Hướng xử lý, khắc phục: Cập nhật bản vá *(đường link bản vá: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26115)*; áp dụng nguyên tắc least privilege (phân quyền tối thiểu) cho các tài khoản database; giới hạn truy cập SQL server qua Firewall, chỉ cho phép các IP tin cậy; bật SQL Server Audit và hệ thống giám sát để kịp thời phát hiện, ngăn chặn hành vi leo thang đặc quyền *(nếu có)*.

1.2. Lỗ hổng CVE-2026-26116 leo thang đặc quyền (Elevation of Privilege - EoP) trong hệ quản trị cơ sở dữ liệu Microsoft SQL Server

- Đánh giá mức độ nghiêm trọng: Cao, điểm CVSS: 8.8/10.

- Mô tả kỹ thuật:

+ Lỗ hổng xuất phát từ việc hệ thống không trung hòa đúng các phần tử đặc biệt trong câu lệnh SQL (CWE-89-SQL injection). Cụ thể, do hệ thống không kiểm tra và xử lý an toàn dữ liệu đầu vào, cho phép kẻ tấn công chèn trực tiếp mã SQL vào truy vấn, từ đó làm thay đổi logic thực thi của cơ sở dữ liệu.

+ Tình huống khai thác: Đối tượng thông qua tài khoản hợp lệ với quyền thấp trong hệ thống SQL Server (ví dụ như tài khoản user ứng dụng), từ đó gửi các truy vấn chứa payload SQL độc hại, do thiếu kiểm tra đầu vào, SQL thực thi các câu lệnh bị chèn, cho phép đối tượng leo thang quyền lên mức cao hơn (db_owner, sysamin), truy cập, sửa đổi các dữ liệu nhạy cảm.

- Phiên bản ảnh hưởng: Các phiên bản SQL Server 2016, 2017, 2019, 2022, 2025 *(chưa được cập nhật, cài đặt bản vá)*.

- Hướng xử lý, khắc phục: Cập nhật bản vá *(đường link bản vá: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26116)*; áp dụng nguyên tắc least privilege (phân quyền tối thiểu) cho các tài khoản database.

2. Lỗ hổng bảo mật trên ứng dụng Microsoft Office

2.1. Lỗ hổng CVE-2026-26110 thực thi mã từ xa (RCE) trên Microsoft Office

- Đánh giá mức độ nghiêm trọng: Cao, điểm CVSS: 8.4/10.

- Mô tả kỹ thuật:

+ Lỗ hổng xuất phát từ lỗi hệ thống xử lý sai kiểu dữ liệu của một đối tượng trong bộ nhớ (type confusion - CWE-843). Khi chương trình xử lý tài

nguyên (tệp tin, đối tượng, dữ liệu) với kiểu không đúng, tin tặc có thể lợi dụng để điều khiển luồng thực thi chương trình.

+ Tình huống khai thác: Đối tượng tạo một tệp Office độc hại (word, excel, Powerpoint), trong đó chứa dữ liệu đặc biệt để gây lỗi xử lý sai kiểu dữ liệu (Type confusion) cho chương trình. Khi người dùng mở tệp trên máy tính, chương trình Office xử lý sai kiểu dữ liệu, dẫn đến kích hoạt, thực thi mã độc do đối tượng chèn, theo đó mã độc được kích hoạt trên máy người dùng, cho phép đối tượng đánh cắp dữ liệu hoặc cài cửa hậu backdoor hoặc mã độc khác.

- Phiên bản ảnh hưởng: Các phiên bản Microsoft 365 Apps 16.0.1 trở về trước, Office 2016 phiên bản 16.0.5543.1000 về trước, Office 2019 phiên bản 19.0.0 về trước, 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-2026-26110)*; không tải về và mở các tệp Office không rõ nguồn gốc; tắt Macro nếu không cần thiết.

2.2. Lỗ hổng CVE-2026-26110 thực thi mã từ xa (RCE) trên Microsoft Office

- Đánh giá mức độ nghiêm trọng: Cao, điểm CVSS: 8.4/10.

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh do lỗi tham chiếu con trỏ không tin cậy (Untrusted Pointer Dereference, xuất phát từ việc chương trình không kiểm tra tính hợp lệ của con trỏ trước khi sử dụng, dẫn đến việc truy cập vào vùng nhớ không tin cậy (CWE-822), khiến ứng dụng xử lý sai dữ liệu trong bộ nhớ, tạo điều kiện cho đối tượng chèn và thực thi mã độc.

+ Tình huống khai thác: Đối tượng tạo lập, tán phát 1 tệp tài liệu Office (Word, excel...) độc hại. Khi người dùng vô tình mở tệp này (hoặc thậm chí chỉ xem qua Preview Pane), lỗ hổng sẽ kích hoạt, cho phép đối tượng thực thi mã độc trên máy người dùng mà không cần quyền trước đó, từ đó cài cắm mã độc, đánh cắp dữ liệu hoặc kiểm soát hệ thống.

- Phiên bản ảnh hưởng: Các phiên bản Microsoft Office 2016, 2019, 365 Apps, Office LTSC 2021/2024, Microsoft Sharepoint Server chưa cài đặt bản vá.

- Hướng xử lý, khắc phục: Cập nhật bản vá *(đường link bản vá: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26113)*; không tải về và mở các tệp Office không rõ nguồn gốc; tắt Preview Pane khi không cần thiết.

3. Các lỗ hổng bảo mật trên ứng dụng trình duyệt Chrome

3.1. Lỗ hổng CVE-2026-3909 ghi tràn bộ nhớ ngoài vùng (Out-of-bounds Write) trên Chrome

- Đánh giá mức độ nghiêm trọng: Cao, điểm CVSS: 8.8/10.

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh từ thư viện đồ họa Skia - một thành phần chịu trách nhiệm xử lý hiển thị hình ảnh, nội dung web và giao diện người dùng. Do lỗi kiểm soát bộ nhớ không chặt chẽ, chương trình cho phép ghi dữ liệu vượt ra ngoài vùng nhớ được cấp phát (CWE-787) dẫn đến khả năng bị lợi dụng khai thác.

+ Tình huống khai thác: Đối tượng tạo lập 01 trang web giả chứa mã độc, khi người dùng vô tình truy cập trang này, lỗ hổng kích hoạt, gây lỗi ghi tràn bộ nhớ, từ đó đối tượng có thể làm hỏng cấu trúc bộ nhớ, dẫn đến treo trình duyệt, rò rỉ dữ liệu hoặc cho phép đối tượng thực thi mã độc ngay trên trình duyệt của người dùng mà không cần quyền truy cập trước.

- Phiên bản ảnh hưởng: Các phiên bản Google Chrome (Chromium-based) trước 146.0.7680.75, Microsoft Edge.

- Hướng xử lý, khắc phục: Cập nhật trình duyệt Chrome phiên bản mới (sau phiên bản 146.0.7680.75/80) để vá lỗi (link bản vá chính thức: https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html); không truy cập vào các đường link, website, shortcut không tin cậy; triển khai các cơ chế bảo vệ bổ sung như sandbox để phát hiện hình vi khai thác.

3.2. Lỗ hổng CVE-2026-3910 thực thi mã từ xa (RCE) trên Chrome

- Đánh giá mức độ nghiêm trọng: Cao, điểm CVSS: 8.8/10.

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh từ việc triển khai sai logic xử lý trong V8 JavaScript Engine, dẫn đến việc quản lý bộ nhớ không an toàn. Khi xử lý các đoạn mã JavaScript hoặc nội dung HTML đặc biệt, Engine có thể ghi hoặc truy cập sai vùng nhớ, tạo điều kiện cho đối tượng tấn công kiểm soát dữ liệu trong bộ nhớ và thực thi mã tùy ý.

+ Tình huống khai thác: Đối tượng tạo lập trang web giả chứa mã JavaScript độc hại, khi người dùng vô tình truy cập trang này, trình duyệt sẽ thực thi mã thông qua V8 và vô tình kích hoạt lỗ hổng. Đối tượng có thể chạy mã độc bên trong môi trường Sandbox trình duyệt, từ đó tiếp tục tìm cách vượt qua lớp bảo vệ sandbox để chiếm quyền kiểm soát máy tính người dùng, đánh cắp dữ liệu.

- Phiên bản ảnh hưởng: Các phiên bản Google Chrome (Chromium-based) trước 146.0.7680.75, Microsoft Edge.

- Hướng xử lý, khắc phục: Cập nhật trình duyệt Chrome phiên bản mới (sau phiên bản 146.0.7680.75/80) để vá lỗi (link bản vá chính thức: https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html); không truy cập vào các đường link, website, shortcut không tin cậy; triển khai các cơ chế bảo vệ Safe Browsing.

3.3. Lỗ hổng bảo mật CVE-2026-0628 thực thi mã từ xa (RCE) tồn tại trên ứng dụng trợ lý ảo Gemini Live của Chrome

- Đánh giá mức độ nghiêm trọng: Cao, điểm CVSS: 8.8/10.

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh do lỗi kiểm soát chính sách, một tiện ích mở rộng (extension) độc hại có thể vượt qua các rào cản bảo mật để chèn các đoạn mã JavaScript hoặc HTML vào các trang có đặc quyền cao hoặc bảng điều khiển Gemini Live. Vì bảng điều khiển Gemini Live là một thành phần của chính trình duyệt, kẻ tấn công có thể chèn mã để khởi động camera và micro mà không cần sự đồng ý của người dùng, truy cập các tệp tin cục bộ, chụp ảnh màn hình các tab trình duyệt và chiếm quyền điều khiển bảng điều khiển để thực hiện một cuộc tấn công lừa đảo.

- Phiên bản ảnh hưởng: Các phiên bản trước 143.0.7499.192.

- Hướng xử lý khắc phục: Nâng cấp Google Chrome lên phiên bản 143.0.7499.192 hoặc cao hơn. Rà soát và gỡ bỏ các tiện ích không rõ nguồn gốc hoặc có yêu cầu quyền truy cập quá rộng.

4. Lỗ hổng bảo mật tồn tại hệ điều hành Ubuntu

**** CVE-2026-3888 leo thang đặc quyền cục bộ (local privilege Escalation)***

- Đánh giá mức độ nghiêm trọng: Cao, điểm CVSS: 7.8/10.

- Phiên bản ảnh hưởng: Các bản cài đặt mặc định của Ubuntu Desktop phiên bản 24.04 trở lên

- Mô tả kỹ thuật:

+ Lỗ hổng này phát sinh từ sự tương tác ngoài ý muốn giữa hai thành phần chuẩn của Ubuntu: snap-confine (công cụ đặc quyền (set-user-ID-root) dùng để thiết lập môi trường sandbox cho các ứng dụng Snap) và systemd-tmpfiles (dịch vụ quản lý và dọn dẹp các tệp tin/thư mục tạm thời trong /tmp).

+ Trong cấu hình mặc định, systemd-tmpfiles sẽ xóa các thư mục tạm không được sử dụng sau một khoảng thời gian (30 ngày trên Ubuntu 24.04 và 10 ngày trên các phiên bản mới hơn). Kẻ tấn công đợi cho đến khi thư mục quan trọng /tmp/.snap (hoặc các đường dẫn liên quan như /tmp/snap-private-tmp/*/tmp/.snap) bị hệ thống dọn dẹp xóa bỏ do quá hạn. Ngay sau khi thư mục bị xóa, kẻ tấn công (với quyền người dùng thấp) sẽ tạo lại thư mục này và đưa vào các tệp tin hoặc symlink độc hại. Khi người dùng hoặc hệ thống khởi chạy một ứng dụng Snap, snap-confine sẽ thực hiện thao tác bind-mount (gắn kết) các tệp tin từ thư mục mà kẻ tấn công đã kiểm soát với quyền root. Điều này cho phép thực thi mã tùy ý hoặc ghi đè các tệp tin hệ thống nhạy cảm, dẫn đến việc chiếm quyền root hoàn toàn.

- Phiên bản ảnh hưởng: Các bản cài đặt mặc định của Ubuntu Desktop phiên bản 24.04 trở lên.

- Hướng xử lý khắc phục: Ubuntu đã phát hành bản vá, người dùng nên cập nhật gói snapd lên phiên bản đã vá lỗi (từ 2.73 trở lên).

5. Các lỗ hổng bảo mật tồn tại trên ứng dụng Secure Firewall Management Center của hãng Cisco

5.1. Lỗ hổng CVE-2026-20131 thực thi mã từ xa

- Đánh giá mức độ nghiêm trọng: Rất cao, điểm CVSS: 10/10.

- Mô tả kỹ thuật: Giao diện quản lý của Secure Firewall Management Center (FMC) xử lý các đối tượng Java (Java objects) do người dùng gửi lên mà không kiểm tra đầy đủ tính xác thực. Kẻ tấn công có thể gửi một "luồng byte Java" (Java byte stream) được thiết kế đặc biệt qua giao thức HTTP/HTTPS. Khi hệ thống FMC nhận và giải mã đối tượng độc hại này, nó sẽ vô tình thực thi các đoạn mã Java tùy ý được chèn bên trong. Cuộc tấn công không yêu cầu bất kỳ quyền đăng nhập nào và kiểm soát toàn bộ hệ thống quản lý, từ đó có thể vô hiệu hóa hàng rào bảo mật của toàn tổ chức.

- Phiên bản ảnh hưởng: Lỗ hổng này tác động diện rộng đến các dòng Cisco chạy phần mềm Secure Firewall Management Center các phiên bản 7.2.x, 7.4.x và 7.6.x (Trước bản vá tháng 03/2026).

- Hướng xử lý khắc phục: Nâng cấp lên phiên bản 7.4.2.3 hoặc 7.6.1.1 trở lên.

5.2. Lỗ hổng CVE-2026-20079 bỏ qua xác thực (Authentication Bypass)

- Đánh giá mức độ nghiêm trọng: Rất cao, điểm CVSS: 10/10.

- Mô tả kỹ thuật:

+ Lỗ hổng Chèn tham số (Argument Injection) cực kỳ nghiêm trọng nằm trong giao diện quản lý dựa trên web của Cisco Secure Firewall Management Center (FMC). Lỗi phát sinh do việc lọc dữ liệu đầu vào không đầy đủ trong các yêu cầu HTTP gửi đến API quản lý. Kẻ tấn công có thể chèn các tham số độc hại vào tiến trình xác thực của hệ thống.

+ Bằng cách gửi một gói tin HTTP được thiết kế đặc biệt, kẻ tấn công có thể "đánh lừa" cơ chế xác thực nội bộ, bỏ qua hoàn toàn bước nhập mật khẩu và được cấp quyền truy cập với vai trò Administrator.

- Phiên bản ảnh hưởng: Lỗ hổng này tác động diện rộng đến các dòng Cisco chạy phần mềm Secure Firewall Management Center các phiên bản 7.2.x, 7.4.x và 7.6.x (Trước bản vá tháng 03/2026).

- Hướng xử lý khắc phục: Nâng cấp lên phiên bản 7.4.2.3 hoặc 7.6.1.1 trở lên. Không bao giờ để giao diện quản lý Secure Firewall Management Center công khai trên internet. Luôn yêu cầu kết nối qua VPN hoặc máy chủ nhảy (Jump Host) có xác thực đa yếu tố (MFA).

6. Lỗ hổng bảo mật tồn tại trên điện thoại Android sử dụng chip Snapdragon *(CVE-2026-21385)*

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

- Mô tả kỹ thuật:

+ Lỗ hổng này nằm trong thành phần Graphics/Display (Đồ họa/Hiển thị) mã nguồn mở của Qualcomm, được sử dụng bởi hầu hết các chipset Snapdragon. Do tràn số nguyên (Integer Overflow) dẫn đến hư hỏng bộ nhớ khi hệ thống thực hiện phân bổ bộ nhớ.

+ Kẻ tấn công có thể lừa người dùng cài đặt một ứng dụng độc hại hoặc thực thi mã cục bộ. Ứng dụng này sẽ gửi dữ liệu được thiết kế đặc biệt đến trình điều khiển đồ họa Snapdragon để làm hỏng bộ nhớ theo cách có kiểm soát. Từ một ứng dụng có quyền hạn thấp có thể chiếm quyền quản trị cao nhất của hệ thống để truy cập trái phép vào dữ liệu nhạy cảm, camera, hoặc microphone.

- Phiên bản ảnh hưởng: Tất cả các điện thoại Android sử dụng chip Snapdragon chưa cập nhật bản vá tháng 03/2026 (đặc biệt là Android 14, 15 và 16).

- Hướng xử lý khắc phục: Cài đặt bản cập nhật Android từ ngày tháng 03/2026 trở về sau.

7. Lỗ hổng bảo mật tồn tại trong plugin WordPres *(CVE-2026-1492)*

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

- Mô tả kỹ thuật:

+ Lỗ hổng này xảy ra do lỗi Quản lý đặc quyền không đúng cách trong plugin User Registration & Membership. Plugin này cho phép người dùng đăng ký tài khoản thành viên qua các biểu mẫu tùy chỉnh. Tuy nhiên, hệ thống lại chấp nhận tham số định danh vai trò (role) do người dùng gửi lên từ phía trình duyệt (client-side) mà không thực hiện kiểm tra đối chiếu với danh sách cho phép (allowlist) ở phía máy chủ.

+ Kẻ tấn công chỉ cần gửi một yêu cầu đăng ký tài khoản thông thường nhưng chèn thêm hoặc thay đổi tham số role thành administrator. Vì thiếu bước xác thực quyền hạn trên server, plugin sẽ mặc định cấp quyền Quản trị viên (Admin) cho tài khoản mới này. Khi đã có quyền Admin, họ có toàn quyền thay đổi nội dung, cài đặt mã độc, đánh cắp dữ liệu người dùng hoặc xóa toàn bộ website. Lỗ hổng này không yêu cầu xác thực, có độ phức tạp thấp và có thể khai thác hàng loạt qua mạng Internet.

- Phiên bản ảnh hưởng: Tất cả các phiên bản Plugin User Registration & Membership từ 5.1.2 trở về trước.

- Hướng xử lý khắc phục: Nâng cấp plugin lên phiên bản 5.1.3 hoặc mới nhất hiện có.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của 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.

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.

Công an tỉnh trao đổi để quý cơ quan phối hợp thực hiện./.

Nơi nhận:
- Như trên (phối hợp);
- UBND tỉnh (báo cáo);
- Đ/c Giám đốc Công an tỉnh (báo cáo);
- Phòng Tham mưu;
- Lưu: VT, ANM.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Nguyễn Thành Long