BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

Số: 479 /CAT-ANM
V/v cảnh báo lỗ hổng bảo mật nghiêm trọng tháng 12/2025

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

Quảng Ngãi, ngày 23 tháng 01 năm 2025

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 12/2025, qua công tác bảo đảm an toàn thông tin, 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 **16** lỗ hổng bảo mật nghiêm trọng ảnh hưởng đến hệ thống thông tin *(Tài liệu lưu hành nội bộ)*. Trong đó có 01 lỗ hổng bảo mật có mức độ nguy hiểm rất cao, 14 lỗ hổng bảo mật mức độ nguy hiểm cao, 01 lỗ hổng bảo mật mức độ nguy hiểm trung bình, cụ thể:

1. Lỗ hổng bảo mật trên hệ điều hành của Microsoft

1.1.* CVE-2025-62554 và CVE-2025-62557 - *Lỗ hổng thực thi mã nghiêm trọng trong Microsoft Office (chung)

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.4/10)

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh trong thành phần xử lý đối tượng và metadata của tài liệu Office. Quá trình phân tích tự động, như quét nội dung hoặc trích xuất thông tin, có thể xử lý sai kiểu đối tượng mà không cần người dùng mở file, dẫn đến thực thi mã.

+ Tình huống khai thác: Một cơ quan có mạng nội bộ có chia sẻ tài liệu Office. Kẻ tấn công tải lên một tệp Office được tạo đặc biệt, theo đó, trong quá trình hệ thống tự động quét hoặc xử lý metadata của tệp độc hại, lỗi xử lý đối tượng có thể bị kích hoạt mà không cần mở file, khiến mã độc được kích hoạt,

chạy trực tiếp trên máy chủ và tạo cửa hậu truy cập lâu dài.

- Phiên bản ảnh hưởng: Các phiên bản Office 2016 trở lên và Microsoft 365 Apps đều bị ảnh hưởng, đặc biệt trên máy chủ xử lý tài liệu.

- Khuyến nghị: Lỗ hổng cần được ưu tiên xử lý ngay lập tức vì nguy cơ khai thác âm thầm và khó phát hiện. Người dùng nên áp dụng bản vá do Microsoft phát hành: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62554; và https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62557

1.2. CVE-2025-62552 - Lỗ hổng thực thi mã trong Microsoft Office Access.

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 7.8/10)

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh từ cơ chế xử lý cấu trúc bảng và dữ liệu nhị phân trong tệp accdb. Khi Access phân tích các bảng hoặc truy vấn có cấu trúc bất thường, việc kiểm tra biên và quản lý bộ nhớ không đầy đủ dẫn đến ghi đè vùng nhớ và thực thi mã. Điều này cho phép kẻ tấn công chèn và thực thi mã tùy ý trong ngữ cảnh người dùng hiện tại khi tệp được mở. Lỗ hổng không yêu cầu đặc quyền trước và có độ phức tạp khai thác thấp, tuy nhiên cần người dùng tương tác mở tệp. Trong môi trường nội bộ, nguy cơ bị khai thác cao nếu người dùng thường xuyên trao đổi file Access qua email hoặc USB.

+ Tình huống khai thác: Kẻ tấn công gửi cho người dùng một tệp Access giả mạo được đặt tên giống biểu mẫu nội bộ. Khi cán bộ mở tệp để xem dữ liệu, mã độc được kích hoạt, âm thầm cài đặt chương trình thu thập thông tin đăng nhập trên máy tính, từ đó tạo điều kiện cho kẻ tấn công xâm nhập sâu hơn vào hệ thống nội bộ.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng các phiên bản Microsoft Office 2016, 2019, 2021 và Microsoft 365 Apps có cài Access, nếu chưa được vá bảo mật.

- Khuyến nghị: Lỗ hổng đặc biệt nguy hiểm với các đơn vị sử dụng Access để lưu trữ dữ liệu nghiệp vụ. Cần vá sớm và hạn chế mở file Access từ nguồn không xác thực. Người dùng nên áp dụng bản vá do Microsoft phát hành: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62552

1.3. Các lỗ hổng thực thi mã trong Microsoft Office Excel

*** CVE-2025-62553**

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 7.8/10)

- Mô tả kỹ thuật:

+ Nguồn gốc lỗ hổng nằm ở quá trình Excel xử lý bảng tính phức tạp, dữ liệu ẩn và công thức được tạo không đúng chuẩn. Khi mở tệp, Excel tự động nạp và tính toán dữ liệu, lỗi kiểm tra biên có thể bị kích hoạt để chạy mã độc. Lỗ hổng yêu cầu người dùng mở file nhưng không cần quyền truy cập đặc biệt, kẻ tấn công có thể lợi dụng để thực thi mã khi người dùng mở tệp Excel độc hại.

- Khuyến nghị: Người dùng nên áp dụng bản vá do Microsoft phát hành:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62560

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62561

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62563

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62564

1.4. Các lỗ hổng thực thi mã trong Microsoft Office Word

*** CVE-2025-62555**

- Đánh giá mức độ nguy hiểm: Trung bình (điểm CVSS: 7.0/10). Tuy mức độ thấp hơn các lỗi khác nhưng vẫn nguy hiểm do Word là định dạng được sử dụng rộng rãi.

- Mô tả kỹ thuật:

+ Nguồn gốc lỗ hổng liên quan đến việc Word xử lý cấu trúc tài liệu phức tạp và dữ liệu nhúng. Khi tài liệu chứa các đối tượng được tạo bất thường, lỗi quản lý vùng nhớ xảy ra và cho phép mã độc chạy với quyền người dùng.

+ Tình huống khai thác: Một tài liệu Word giả mạo thông báo nội bộ được gửi đến nhiều cán bộ. Khi mở file, mã độc kích hoạt, cho phép kẻ tấn công theo dõi bàn phím và chụp màn hình.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng Word 2016, 2019, 2021 và Microsoft 365 Apps.

- Khuyến nghị: Lỗ hổng phù hợp với các chiến dịch tấn công diện rộng. Cần áp dụng chế độ Protected View và chặn file Word từ nguồn lạ. Người dùng nên áp dụng bản vá do Microsoft phát hành: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62555

*** CVE-2025-62558 và CVE-2025-62559**

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 7.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh từ cơ chế xử lý đối tượng OLE và nội dung nhúng trong tài liệu Word. Khi mở file chứa đối tượng được tạo đặc biệt, Word xử lý sai cấu trúc dữ liệu và cho phép thực thi mã.

+ Tình huống khai thác: Người dùng trao đổi tài liệu với đối tác qua email. Kẻ tấn công gửi file Word giả mạo chứa đối tượng OLE độc hại. Khi người dùng mở file, Word xử lý sai các đối tượng nhúng, kích hoạt lỗ hổng và khiến ransomware chạy ngay lập tức, mã hóa toàn bộ tài liệu trên máy.

- Phiên bản ảnh hưởng: Word từ 2016 trở lên.

- Khuyến nghị: Người dùng nên áp dụng bản vá do Microsoft phát hành:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62558;

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62559

+ Tình huống khai thác: Kẻ tấn công giả mạo lãnh đạo, cán bộ gửi file Excel có cấu trúc bảng bất thường. Khi người dùng mở file, Excel xử lý dữ liệu và phát sinh lỗi kiểm tra biên, khiến mã độc chạy ngầm, dẫn đến việc máy tính bị cài công cụ điều khiển từ xa và bị lợi dụng để dò quét mạng nội bộ.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng Excel trong Office 2016, 2019, 2021 và Microsoft 365 Apps.

- Khuyến nghị: Lỗ hổng thường được sử dụng trong các chiến dịch câu nhử phishing. Cần tăng cường nhận thức người dùng và cập nhật bản vá đầy đủ. Người dùng nên áp dụng bản vá do Microsoft phát hành: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62553

*** CVE-2025-62556**

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 7.8/10)

- Mô tả kỹ thuật:

+ Lỗ hổng xuất phát từ việc Excel xử lý dữ liệu trong các tệp được chia sẻ qua mạng nội bộ hoặc thư mục dùng chung. Việc thiếu kiểm tra tính toàn vẹn dữ liệu đầu vào có thể dẫn đến thực thi mã khi người dùng mở file.

+ Tình huống khai thác: File Excel được tải về từ trang chia sẻ dữ liệu nội bộ nhưng đã bị thay thế bằng phiên bản chứa mã độc. Người dùng mở file và hệ thống bị cài phần mềm gián điệp.

- Phiên bản ảnh hưởng: Các phiên bản Excel thuộc Office 2016 trở lên đều bị ảnh hưởng nếu chưa cập nhật.

- Khuyến nghị: Người dùng nên áp dụng bản vá do Microsoft phát hành: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62556

*** CVE-2025-62560, CVE-2025-62561, CVE-2025-62563, CVE-2025-62564**

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 7.8/10)

- Mô tả kỹ thuật:

+ Các lỗ hổng này phát sinh từ quá trình Excel xử lý bảng dữ liệu lớn, công thức phức tạp, dữ liệu ẩn, liên kết và tham chiếu giữa các ô. Khi tệp Excel được thiết kế với dữ liệu bất thường, việc kiểm tra biên, kiểm soát kiểu dữ liệu và quản lý bộ nhớ không đầy đủ có thể gây lỗi bộ nhớ, cho phép mã độc được thực thi trong ngữ cảnh người dùng khi mở tệp. Trong một số trường hợp, mã độc còn có khả năng tải thêm thành phần tấn công từ bên ngoài, làm gia tăng mức độ xâm nhập.

+ Tình huống khai thác: Kẻ tấn công gửi file Excel giả mạo có nội dung giống file thật. Khi người dùng mở file, Excel xử lý công thức và dữ liệu ẩn bị lỗi, kích hoạt mã độc tải thêm thành phần tấn công, dẫn đến việc thông tin dữ liệu cá nhân bị đánh cắp.

- Phiên bản ảnh hưởng: Các lỗ hổng này ảnh hưởng đến Microsoft Office Excel thuộc Office 2016, 2019, 2021 và Microsoft 365 Apps, đặc biệt nguy hiểm trong môi trường thường xuyên chia sẻ và xử lý tệp Excel nội bộ.

1.5. CVE-2025-62562 - Lỗ hổng thực thi mã trong Microsoft Office Outlook

- Đánh giá mức độ nguy hiểm: Trung bình (điểm CVSS: 7.8/10).

- Mô tả kỹ thuật:

+ Lỗ hổng phát sinh từ cơ chế hiển thị và phân tích nội dung email, đặc biệt ở chế độ xem trước. Outlook xử lý nội dung HTML hoặc đối tượng nhúng không an toàn, cho phép mã độc chạy nền khi email được hiển thị.

+ Tình huống khai thác: Người dùng sử dụng Outlook với chế độ xem trước email. Kẻ tấn công gửi email chứa nội dung hoặc tệp đính kèm được thiết kế đặc biệt *(kèm payload)*. Ngay khi email được hiển thị, Outlook xử lý dữ liệu và kích hoạt lỗ hổng, khiến mã độc chạy nền, cài backdoor và cho phép theo dõi, thu thập thông tin email trong thời gian dài.

- Phiên bản ảnh hưởng: Lỗ hổng ảnh hưởng các phiên bản Outlook 2016 trở lên và Microsoft 365 Apps.

- Khuyến nghị: Người dùng nên áp dụng bản vá do Microsoft phát hành: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-62562

2. Lỗ hổng bảo mật thiết bị mạng D-Link

**** CVE-2026-0625 - Lỗ hổng bảo mật chưa được vá (zero-day) trên các thiết bị phát wifi D-Link đã ngừng sản xuất***

- Đánh giá mức độ nguy hiểm: Rất cao (điểm CVSS: 9.3/10).

- Mô tả kỹ thuật: Lỗ hổng xuất phát từ việc dữ liệu đầu vào không được kiểm tra và lọc chặt chẽ, khiến các tham số cấu hình hệ thống phân giải tên miền (DNS) có thể bị lợi dụng để chèn lệnh "Shell" trực tiếp vào hệ thống; điều nguy hiểm hơn là kẻ tấn công không cần đăng nhập, chỉ cần truy cập được vào thiết bị đầu cuối là có thể thực thi mã từ xa. Khi khai thác thành công, tin tặc có thể thực thi lệnh từ xa không cần xác thực; chiếm quyền có thể khiến toàn bộ thiết bị trong mạng nội bộ bị theo dõi, tấn công hoặc đánh cắp dữ liệu mà người dùng không hay biết hoặc biến thiết bị thành một phần của botnet.

- Phiên bản ảnh hưởng: DSL-526B, DSL-2640B, DSL-2740R, DSL-2780B; các thiết bị này đều đã hết vòng đời từ năm 2020, đồng nghĩa với việc không còn bản vá, cập nhật bảo mật hay hỗ trợ kỹ thuật từ hãng sản xuất.

- Khuyến nghị: Ngừng sử dụng ngay các thiết bị D-LINK đời cũ, thay thế bằng thiết bị còn được hãng hỗ trợ; không bật quản trị từ xa nếu không thật sự cần.

3. Lỗ hổng bảo mật trên trình duyệt Chrome

****CVE-2025-14765 - Lổ hổng quản lý bộ nhớ không an toàn, cho phép kẻ tấn công thao túng vùng nhớ đã bị giải phóng và từ đó thực thi mã từ xa***

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.8/10).

- Mô tả kỹ thuật: Lỗ hổng bảo mật cho phép thực thi mã từ xa (RCE) mà không cần quyền quản trị thông qua lỗi Use-After-Free (UAF) trong WebGPU; lợi dụng việc quản lý bộ nhớ không an toàn, cho phép kẻ tấn công thao túng vùng nhớ đã bị giải phóng, từ đó chiếm quyền kiểm soát trình duyệt.

- Phiên bản ảnh hưởng: Google Chrome các phiên bản cũ hơn 143.0.7499.146 (trên Windows, Mac, Linux và Android).

- Khuyến nghị: Nâng cấp lên phiên bản Chrome 143.0.7499.146 hoặc cao hơn. Vào "Cài đặt" -> "Giới thiệu về Chrome" -> Chờ tải bản vá -> Nhấn Relaunch để hoàn tất.

4. Lỗ hổng bảo mật trên trình hệ quản trị cơ cơ sở dữ liệu MongoDB

CVE-2025-14847 – Lỗ hổng hưởng đến giao thức nén Zlib và cho phép kẻ tấn công đọc bộ nhớ heap chưa được khởi tạo mà không cần xác thực

- Đánh giá mức độ nguy hiểm: Cao (điểm CVSS: 8.7/10).

- Mô tả kỹ thuật: Lỗ hổng cho phép rò rỉ dữ liệu nhạy cảm từ bộ nhớ mà không cần xác thực. Kẻ tấn công chỉ cần có kết nối mạng tới cổng dịch vụ của MongoDB (mặc định là 27017) là có thể khai thác. Lỗi phát sinh từ việc xử lý không khớp độ dài giữa tiêu đề (header) gói tin nén và dữ liệu thực tế. Kẻ tấn công gửi một gói tin OP_COMPRESSED với tham số uncompressedSize được tùy chỉnh lớn hơn thực tế. Máy chủ MongoDB sẽ cấp phát một vùng đệm bộ nhớ quá lớn và trả về toàn bộ vùng nhớ đó (bao gồm cả các dữ liệu "rác" còn sót lại từ các tác vụ trước) cho kẻ tấn công. Những dữ liệu này thường chứa mật khẩu văn bản thô, khóa API, session tokens và các bản ghi dữ liệu nhạy cảm.

- Phiên bản ảnh hưởng: Lỗ hổng này có phạm vi ảnh hưởng rất rộng, bao gồm hầu hết các phiên bản được phát hành trong gần 10 năm qua:

+ Dòng 8.2, các phiên bản cũ hơn 8.2.3.

+ Dòng 8.0 , các phiên bản cũ hơn 8.0.17.

+ Dòng 7.0, các phiên bản cũ hơn 7.0.28.

+ Dòng 6.0, các phiên bản cũ hơn 6.0.27.

+ Dòng 5.0, các phiên bản cũ hơn 5.0.32.

+ Dòng 4.4, các phiên bản cũ hơn 4.4.30.

+ Các dòng cũ (EOL): Toàn bộ dòng 4.2, 4.0 và 3.6 đều bị ảnh hưởng và không có bản vá chính thức do đã hết vòng đời hỗ trợ.

- Khuyến nghị:

+ Nâng cấp bản vá, ưu tiên số một là cập nhật lên phiên bản mới nhất của dòng đang sử dụng (ví dụ: 8.0.17 hoặc 7.0.28).

+ Cấu hình tạm thời: Nếu chưa thể cập nhật ngay, hãy vô hiệu hóa trình nén zlib bằng cách thay đổi cấu hình net.compression.compressors sang các chuẩn khác như snappy hoặc zstd, hoặc tắt hoàn toàn tính năng nén mạng.

+ Thắt chặt bảo mật mạng: Đảm bảo máy chủ MongoDB nằm trong mạng nội bộ, sử dụng Firewall để chặn truy cập từ IP lạ và bắt buộc sử dụng TLS/SSL.

- Mã khai thác Proof of Concept (PoC) đã được công bố rộng rãi trên GitHub và các diễn đàn bảo mật trong tháng 12/2025.

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, cập nhật, vá lỗi hệ thống, 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);
- Giám đốc Công an tỉnh;
- Phòng Tham mưu;
- Lưu: VT, ANM.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
CÔNG AN TỈNH QUẢNG NGÃI

Đại tá Võ Văn Dương