BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

Số: 3390/CAT-ANM

V/v cảnh báo lỗ hổng bảo mật đặc biệt nghiêm trọng tồn tại trên các nền tảng ASP.NET Core, DotNetNuke

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

Quảng Ngãi, ngày 18 tháng 11 năm 2025

Kính gửi:
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Văn phòng Tỉnh ủy, văn phòng 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;
- UBND các xã, phường, Đặc khu Lý Sơn.
- 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;

Qua công tác bảo đảm an toàn thông tin, an ninh mạng trên địa bàn tỉnh, lực lượng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao phát hiện **02** lỗ hổng bảo mật đặc biệt nghiêm trọng ảnh hưởng đến hoạt động của hệ thống thông tin của các cơ quan Đảng, Nhà nước, tổ chức, doanh nghiệp trên địa bàn tỉnh *(có Phục lục kèm theo)*:

(1) Lỗ hổng trong nền tảng ASP.NET Core (là công nghệ mã nguồn mở phổ biến được sử dụng để xây dựng các website và dịch vụ trực tuyến trên không gian mạng) có mã định danh CVE-2025-55315 với điểm CVSS 9,9/10; cho phép kẻ tấn công khai thác kỹ thuật HTTP Request Smuggling, khiến hệ thống xử lý sai lệch các yêu cầu HTTP và vô hiệu hóa các cơ chế bảo mật;

(2) Lỗ hổng trong nền tảng DotNetNuke (là nền tảng quản trị nội dung và xây dựng các ứng dụng website) có mã định danh CVE-2025-64095 với điểm CVSS 10/10; cho phép tải tập lên mà không cần xác thực trên nền tảng quản lý nội dung, ảnh hưởng các phiên bản trước 10.1.1. Lỗ hổng nằm ở trình soạn thảo HTML mặc định, nơi kiểm tra và xác minh việc tải tập chưa được thực hiện đúng cách, cho phép kẻ tấn công tải các tập độc hại hoặc ghi đè lên các tập quan trọng trên hệ thống mà không cần thông tin đăng nhập.

Với khả năng khai thác lỗ hổng bảo mật và mức độ ứng dụng phổ biến của các nền tảng ASP.NET Core, DotNetNuke trong các hệ thống thông tin dễ dàng

tiềm ẩn nguy cơ để tin tặc lợi dụng lỗ hổng bảo mật thực hiện tấn công mạng vào các hệ thống thông tin quan trọng của cơ quan Đảng, Nhà nước, tổ chức, doanh nghiệp hoặc thực hiện các hành vi xâm phạm an ninh quốc gia, trật tự an toàn xã hội.

Nhằm bảo đảm an toàn thông tin, an ninh mạng cho hệ thống thông tin của các cơ quan Đảng, Nhà nước, tổ chức, doanh nghiệp trên địa bàn tỉnh, Công an tỉnh đề nghị lãnh đạo các cơ quan, đơn vị chỉ đạo thực hiện:

1. Kiểm tra, rà soát và xác định các lỗ hổng bảo mật trong hệ thống thông tin; khẩn trương triển khai thực hiện giải pháp khắc phục, xử lý theo các khuyến nghị tại Phục lục kèm theo.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh báo kịp thời của các cơ quan chức năng và các tổ chức lớn về an ninh mạng để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Trong trường hợp phát hiện dấu hiệu tấn công mạng khai thác lỗ hổng bảo mật trên, đề nghị các đơn vị liên hệ Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, điện thoại: 0888.309.485, thư điện tử: anm-ca@quangngai.gov.vn) để báo cáo sự cố và được hướng dẫn hỗ trợ.

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

Nơi nhận:
- Như trên;
- Giám đốc Công an tỉnh (báo cáo);
- Công an các đơn vị, địa phương;
- Lưu: VT, ANM.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Võ Văn Dương

PHỤC LỤC
THÔNG TIN VỀ CÁC LỖ HỔNG ĐẶC BIỆT NGHIÊM TRỌNG CVE-2025-53770 VÀ CVE-2025-64095

(Kèm theo Công văn số 3790/CAT-ANM ngày 18 /11/2025 của Công an tỉnh)

Tài liệu lưu hành nội bộ

1. Lỗ hổng bảo mật trên nền tảng ASP.NET Core (CVE-2025-55315)

- Lỗ hổng mang mã định danh CVE-2025-55315.

- Điểm CVSS: 9,9/10.

- Mức độ: Đặc biệt nghiêm trọng.

- Mô tả lỗ hổng:

+ HTTP Request Smuggling khai thác sự khác biệt trong cách proxy, load balancer và máy chủ backend hiểu tiêu chuẩn HTTP. Khi các tiêu đề như Content-Length và Transfer-Encoding mâu thuẫn, từng lớp có thể diễn giải luồng dữ liệu khác nhau, tạo cơ hội cho kẻ tấn công giấu một yêu cầu ẩn trong luồng hợp lệ. Trong hạ tầng hiện đại, nơi CDN, proxy và nhiều lớp cân bằng tải cùng tham gia định tuyến, một yêu cầu bị "smuggle" có thể trượt qua các lớp trung gian và chạm tới logic ứng dụng mà khó phát hiện qua log, biến lỗi tầng vận chuyển thành cửa hậu trên tầng ứng dụng.

+ Lỗ hổng này đặc biệt nguy hiểm vì không yêu cầu quyền truy cập hay tương tác từ người dùng, cho phép kẻ tấn công tự động hóa khai thác trên diện rộng. Những tổ chức xử lý dữ liệu nhạy cảm như ngân hàng, bệnh viện hay cơ quan quản lý thông tin cá nhân trở thành mục tiêu hàng đầu, bởi một lần tấn công thành công có thể dẫn đến rò rỉ dữ liệu, chiếm đoạt phiên người dùng hoặc leo quyền quản trị.

- Khuyến nghị: Kiểm tra, rà soát và xác định lỗ hổng trong các giải pháp sử dụng nền tảng ASP.NET Core. Thực hiện cập nhật bản vá bảo mật cho các máy bị ảnh hưởng theo hướng dẫn của Microsoft *(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-55315)*

2. Lỗ hổng bảo mật trên nền tảng DotNetNuke (CVE-2025-64095)

- Lỗ hổng mang mã định danh CVE-2025-64095.

- Điểm CVSS: 10/10;.

- Mức độ: Đặc biệt nghiêm trọng;.

- Mô tả lỗ hổng:

+ Lỗ hổng phép tải tập lên mà không cần xác thực trên nền tảng quản lý nội dung web phổ biến DotNetNuke phiên bản trước 10.1.1. Lỗ hổng nằm ở trình soạn thảo HTML mặc định, nơi kiểm tra và xác minh việc tải tập chưa

được thực hiện đúng cách, cho phép kẻ tấn công tải các tập độc hại hoặc ghi đè lên các tập quan trọng trên hệ thống mà không cần thông tin đăng nhập.

+ Kẻ tấn công có thể thay đổi giao diện website (defacement), chèn các mã độc hoặc thực hiện các cuộc tấn công Stored Cross-Site Scripting (Stored-XSS), dẫn tới mất kiểm soát nội dung và ảnh hưởng nghiêm trọng đến người dùng cuối.

+ Ước tính số lượng máy chủ kết nối Internet và sử dụng DotNetNuke có thể bị ảnh hưởng trên toàn cầu dao động từ khoảng **15.000 đến 18.000**. Tại Việt Nam có khoảng **400-500** máy chủ công khai trên Internet sử dụng nền tảng này. Trong đó hơn **50%** là các máy chủ đang được triển khai trong **các cơ quan, đơn vị nhà nước**.

+ Các hệ thống dễ bị tổn thương thường là các trang thông tin công khai, các cổng truy cập khách hàng, đối tác, hệ thống nội bộ công khai ra bên ngoài, hoặc các phiên bản DotNetNuke cũ được lưu trữ trên hạ tầng không được quản lý chặt chẽ.

- Khuyến nghị: Mặc dù chưa có báo cáo về việc khai thác rộng rãi lỗ hổng này, nhưng do tính chất dễ khai thác và đã có nhiều hoạt động quét trên diện rộng nhằm xác định các hệ thống dễ bị tổn thương, mọi tổ chức có hệ thống DotNetNuke chưa được vá cần đặc biệt cảnh giác và xử lý nhanh chóng để ngăn ngừa nguy cơ bị tấn công. Kiểm tra, rà soát và xác định lỗ hổng trong các giải pháp sử dụng nền tảng DotNetNuke. Thực hiện cập nhật bản vá bảo mật lên DotNetNuke 10.1.1 trở lên./.