BỘ CÔNG AN
CÔNG AN TỈNH ĐẮK NÔNG

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

Số: 2607/CAT-PA05

Đắk Nông, ngày 26 tháng 11 năm 2024

V/v cảnh báo nguy cơ mất an ninh, an toàn thông tin đối với trang thông tin điện tử sử dụng mã nguồn NukeViet

Kính gửi:
- Các Sở, ban, ngành tỉnh Đắk Nông;
- Ủy ban nhân dân các huyện, thành phố.

Qua công tác giám sát an ninh mạng, Công an tỉnh phát hiện lỗ hổng bảo mật nghiêm trọng tồn tại trên một số trang thông tin điện tử có sử dụng mã nguồn mở NukeViet của các đơn vị, địa phương trên cả nước, trong đó có các trang thông tin điện tử của các đơn vị trên địa bàn tỉnh Đắk Nông. Các lỗ hổng bảo mật này tiềm ẩn nguy cơ cao bị các đối tượng tin tặc tấn công xâm nhập chiếm quyền điều khiển, cụ thể thông tin lỗ hổng bảo mật như sau:

Lỗ hổng bảo mật CVE-2019-7726 tồn tại trong mã nguồn NukeViet CMS trước phiên bản 4.3.04 cho phép đối tượng tấn công thực hiện câu lệnh truy vấn SQL tùy ý bằng cách gửi dữ liệu không cần được kiểm tra đầu vào đến ứng dụng. Thông qua lỗ hổng này, tin tặc có thể khai thác để xâm nhập vào cơ sở dữ liệu, truy cập, thay đổi hoặc xóa thông tin. Nghiêm trọng hơn, nếu kết hợp với các kỹ thuật tấn công khác, lỗ hổng này có thể dẫn đến việc chiếm quyền kiểm soát hoàn toàn hệ thống. Mặc dù đơn vị phát triển mã nguồn NukeViet đã công khai lỗ hổng và phát hành bản vá từ năm 2020, song đến thời điểm hiện tại vẫn còn nhiều đơn vị chủ quản chưa tiến hành cập nhật bản vá, dẫn đến nguy cơ bị tin tặc khai thác lỗ hổng để cài cắm mã độc, chiếm quyền quản trị trang thông tin điện tử và máy chủ website lưu trữ trang thông tin điện tử.

Các trang thông tin điện tử trên địa bàn tỉnh là nơi đăng tải các thông báo, tin tức chính thống của chính quyền địa phương, có lượng truy cập cao của quần chúng nhân dân, khi bị tin tặc chiếm quyền quản trị các trang thông tin điện tử này sẽ thực hiện hành vi tùy ý thay đổi nội dung tin tức, hình ảnh, đăng tải các thông tin sai lệch, thậm chí điều hướng đến các website độc hại nhằm phát tán thông tin xấu độc, sai sự thật phá hoại nền tảng tư tưởng của Đảng, chống phá Đảng, Nhà nước hoặc thực hiện hành vi phạm pháp luật trên không gian mạng, phát tán mã độc. Nghiêm trọng hơn, hệ thống thông tin của các tỉnh, thành phố thường có cơ chế liên kết, đồng bộ dữ liệu giữa các cơ quan, đơn vị trong cùng địa phương hoặc ngành dọc, thậm chí được cài đặt trên cùng một dải mạng, do đó sau khi chiếm được quyền quản trị máy chủ lưu trữ trang thông tin điện tử, tin tặc

có thể kết hợp khai thác lỗ hổng đã nêu với các kỹ thuật tấn công khác để leo thang đặc quyền xâm nhập, phá hoại, trích xuất dữ liệu từ các hệ thống thông tin khác của đơn vị trên địa bàn tỉnh, dẫn đến nguy cơ lộ, mất bí mật nhà nước.

Trước tình hình trên, để tăng cường công tác đảm bảo an ninh mạng, an toàn thông tin, phòng ngừa tấn công mạng, Công an tỉnh Đắk Nông khuyến cáo các đơn vị thực hiện một số biện pháp như sau:

1. Kiểm tra, rà soát hệ thống thông tin, đặc biệt là các trang tin, cổng thông tin điện tử nếu có sử dụng hệ quản trị nội dung NukeViet trước phiên bản 4.3.04 cần chủ động cập nhật nâng cấp mã nguồn NukeViet CMS lên phiên bản cao hơn và tiến hành đánh giá xâm nhập hệ thống *(Compromise Assessment)*; đồng thời sử dụng mật khẩu mạnh cho các tài khoản quản trị, biên tập trên trang nhằm tránh bị tấn công vét cạn.

2. Chủ động công tác giám sát và chuẩn bị sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; thường xuyên theo dõi cập nhật, phổ biến các văn bản cảnh báo của các cơ quan chức năng và nhà cung cấp sản phẩm, thiết bị an ninh mạng để kịp thời phát hiện, ngăn chặn các nguy cơ tấn công mạng.

3. Trong trường hợp nghi ngờ hoặc phát hiện dấu hiệu tấn công mạng, cần báo cáo ngay về Đội Ứng cứu sự cố tỉnh và Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)* để phối hợp xử lý, khắc phục, ứng cứu sự cố.

Công an tỉnh thông báo đến các đơn vị biết phối hợp, thực hiện./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc CAT (để báo cáo);
- Tiểu ban An toàn an ninh mạng (để theo dõi);
- Đội Ứng cứu sự cố tỉnh (để theo dõi);
- Phòng PV01 (để theo dõi);
- Lưu: VT, PA05 (Đ3).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG AN TỈNH ĐẮK NÔNG

Đại tá Hồ Quang Thắng