

Tin tặc sẽ tiếp tục nhắm tới việc khai thác các lỗ hổng mức độ cao trong các tháng cuối năm

09:51 16/08/2023

Mới đây, Công ty An ninh mạng Viettel - Viettel Cyber Security (VCS) đã có báo cáo về các lỗ hổng bảo mật được tin tặc khai thác trong nửa đầu năm nay...



Ảnh minh họa

Theo đó, quá trình giám sát không gian mạng Việt Nam, hệ thống kỹ thuật của Viettel Cyber Security đã ghi nhận nhiều cuộc tấn công lợi dụng các lỗ hổng nghiêm trọng trên các sản phẩm phổ biến được sử dụng để làm bàn đạp cho các nhóm tin tặc bước đầu xâm phạm hệ thống và thực thi các hành vi độc hại tiếp theo.

Thống kê của Viettel Cyber Security về tỷ lệ các lỗ hổng bảo mật được tin tặc sử dụng trong các chiến dịch tấn công thực tế vào hệ thống tại Việt Nam 6 tháng đầu năm cho thấy, chiếm phần lớn là các lỗ hổng tồn tại trong mã nguồn trang web và các lỗ hổng nghiêm trọng từ các năm trước trong các sản phẩm CNTT phổ biến. Nổi bật, có thể kể tới các lỗ hổng CVE-2020-7961, CVE-2019-16891, CVE-2019-18935, CVE-2017-9248, CVE-2022-41040 hay CVE-2022-41082.

Các chuyên gia Viettel Cyber Security cũng dự báo rằng trong các tháng cuối năm nay, các nhóm tin tặc vẫn sẽ tiếp tục nhắm tới việc khai thác các lỗ hổng đã được công bố với mức độ cao, nghiêm trọng trên các sản phẩm phổ biến như CMS, email server, các giải pháp bảo mật, các nền tảng quản lý công việc... Cùng với đó, các nhóm tấn công còn khai thác, sử dụng những lỗ hổng bảo mật mới được công bố.

Để phòng tránh, các chuyên gia khuyến nghị quản trị viên cần nắm thông tin kịp thời, cập nhật và thực hiện các biện pháp bảo mật cho hệ thống để đảm bảo an toàn thông tin cho đơn vị, tổ chức mình.

Đề cập đến nguy cơ bị tấn công mạng từ khai thác lỗ hổng bảo mật, Cục An toàn thông tin nhận định, trong quá trình chuyển đổi số, số lượng các ứng dụng, hệ thống thông tin của các tổ chức, doanh nghiệp ngày càng nhiều. Do vậy, các lỗ hổng và nguy cơ tấn công mạng thông qua các lỗ hổng bảo mật mới cũng xuất hiện thường xuyên hơn.

Thời gian qua, nhiều biện pháp đã và đang được Cục An toàn thông tin triển khai để góp phần ngăn ngừa các nguy cơ từ những điểm yếu, lỗ hổng của hệ thống, phần mềm như: Triển khai đánh giá, xác định các lỗ hổng bảo mật có mức độ nguy hiểm cao, ảnh hưởng trên diện rộng để hướng dẫn các bộ, ngành cách khắc phục; Chỉ đạo kiểm tra, giám sát trực tiếp và từ xa cho hệ thống thông tin của cơ quan tổ chức.

Cục An toàn thông tin cũng thường xuyên theo dõi, cập nhật cảnh báo an toàn thông tin cho các cơ quan, tổ chức tại Cổng thông tin Khonggianmang.vn, bao gồm việc cảnh báo điểm yếu, lỗ hổng; xây dựng các phương án ứng cứu khẩn cấp, hỗ trợ và khắc phục sự cố trong trường hợp xảy ra tấn công mạng.

Đồng thời, đẩy mạnh tuyên truyền, nâng cao nhận thức cơ bản kỹ năng về an toàn thông tin mạng; đào tạo, bồi dưỡng cho nhân sự chuyên trách an toàn thông tin của cơ quan nhà nước; tổ chức diễn tập thực chiến quy mô quốc gia hàng năm, mời bộ, ngành, địa phương tham gia.

Ngoài ra, việc liên kết, tiếp nhận, trao đổi thông tin với các cơ quan, tổ chức, doanh nghiệp an toàn thông tin trong và ngoài nước để kịp thời nắm bắt các xu hướng, thông tin cũng là một giải pháp được Cục An toàn thông tin chú trọng.

Theo thống kê, hiện đã có 88 đơn vị gồm 63 tỉnh, thành phố và 25 bộ, ngành triển khai giải pháp phòng chống mã độc tập trung và thực hiện kết nối chia sẻ thông tin về mã độc với NCSC.

Số bộ, ngành, địa phương đã triển khai giám sát an toàn thông tin và thực hiện kết nối chia sẻ dữ liệu giám sát với NCSC là 87, gồm 63 tỉnh, thành phố và 24 bộ, ngành.

Hà Trần