

Cảnh báo khẩn cấp: Samsung phát hành bản vá cho lỗ hổng zero-day nguy hiểm

10:56 15/09/2025

Gã khổng lồ công nghệ Samsung vừa phát hành bản vá khẩn cấp cho người dùng điện thoại Galaxy sau khi phát hiện một lỗ hổng zero-day nguy hiểm đang bị tội phạm mạng khai thác ngoài thực tế. Lỗ bảo mật này, có mã định danh là CVE-2025-21043, cho phép kẻ tấn công thực thi mã độc từ xa và truy cập trái phép vào dữ liệu cá nhân của người dùng.



Samsung phát hành bản vá cho lỗ hổng zero-day nguy hiểm

Lỗ hổng nguy hiểm từ thư viện hình ảnh và rủi ro trên diện rộng

Theo Samsung, lỗ hổng zero-day này được phát hiện trong phần mềm xử lý hình ảnh của bên thứ ba có tên libimagecodec.quram. Điều đáng lo ngại là lỗ hổng này lại được ứng dụng WhatsApp (với hơn 3 tỷ người dùng) báo cáo, và WhatsApp là ứng dụng được cài đặt sẵn trên hầu hết các thiết bị Galaxy. Điều này khiến phạm vi tấn công tiềm tàng trở nên lớn hơn bao giờ hết, đe dọa hàng triệu người dùng trên toàn cầu.

Chuyên gia bảo mật Brian Thornton từ Zimperium nhận định: “Lỗ hổng zero-day này cho thấy, tội phạm mạng đang chuyển hướng sang các thiết bị di động như

một mục tiêu tấn công nhanh chóng. Trong trường hợp này, một thư viện nguồn đóng lại tạo ra rủi ro trên diện rộng.”

Samsung xác nhận, các thiết bị chạy Android 13 trở lên đều có nguy cơ bị ảnh hưởng. Hiện cả Samsung và WhatsApp đã phát hành bản vá, nhưng quá trình triển khai trên thực tế lại tương đối phức tạp. Không giống như Apple có thể cập nhật đồng loạt cho hệ điều hành iOS trên toàn cầu, các thiết bị Galaxy phải chờ phát hành theo model, khu vực và nhà mạng. Điều này có nghĩa là nhiều người dùng có thể phải mất thêm thời gian mới nhận được bản sửa lỗi, trong khi rủi ro vẫn đang hiện hữu.

Google đổi chiến lược, Samsung cần cập nhật ngay

Gần đây, Google đã công bố một mô hình phân phối bản vá mới. Thay vì tung ra gói vá hàng tháng bao gồm tất cả các lỗi, hãng sẽ tách riêng các bản vá quan trọng như zero-day để phát hành ngay lập tức. Các lỗi nhỏ hơn sẽ được gộp lại và phát hành theo quý. Cách tiếp cận này được kỳ vọng sẽ giúp các nhà sản xuất, trong đó có Samsung, đẩy nhanh tốc độ cập nhật những lỗi nghiêm trọng.

Nếu Samsung không điều chỉnh, người dùng Galaxy có thể sẽ chỉ nhận được các bản vá quan trọng hai tháng một lần, thay vì cập nhật liên tục như trên Pixel hay iPhone. Trong lúc chờ đợi, các chuyên gia khuyến cáo, người dùng điện thoại Samsung nên kiểm tra cập nhật thường xuyên trong phần Cài đặt - Cập nhật phần mềm. Đồng thời, người dùng cũng nên hạn chế cài đặt các ứng dụng ngoài từ những nguồn không rõ ràng để tự bảo vệ mình.

Nivedita Murthy, một chuyên gia từ Black Duck, nhấn mạnh: “Lỗ hổng này có thể bị lợi dụng để chiếm quyền điều khiển thiết bị và truy cập dữ liệu lưu trữ trên đó. Cập nhật sớm là cách duy nhất để người dùng tự bảo vệ mình.”

Tâm An (t/h)