MCAFEE PHÁT HIỆN 3 LỖI ZERO-DAY OFFICE MỚI

Các ch

Các chuyên gia bảo mật của McAfee cho biết họ lại vừa phát hiện được ba lỗi bảo mật mới chưa được vá trong bộ ứng dụng văn phòng Microsoft Office.

Thông tin đăng tải trên McAfee Avert Labs Blog ngày hôm qua (10/4) thông tin về những lỗi bảo mật nói trên đã được đăng tải trên một số diễn đàn bảo mật. Trong số này có những lỗi có thể bị lợi dụng để thực thi mã độc từ xa.

Kết quả điều tra bước đầu cho thấy trong những lỗi bảo mật nói trên có một lỗi cho phép tấn công từ chối dịch vụ. Điều này đồng nghĩa với việc Office có thể bị treo cứng nếu bị tấn công.

"Đó là một lỗi tràn bộ nhớ đệm. Lỗi này có thể bị khai thác để từ xa thực thi mã độc trên hệ thống mục tiêu," chuyên gia nghiên cứu bảo mật Karthik Raman cho biết. Hình thức tấn công chủ yếu sẽ là phát tán một tệp tin Office có cấy mã khai thác lỗi và lừa người dùng mở nó ra.

McAfee Avert Labs cho biết đang tiến hành nghiên cứu thêm những lỗi trên. Đây cũng là khẳng định của đại diện Microsoft trong một tuyên bố gửi đi hôm qua. Microsoft hiện chưa ghi nhận được bất kỳ một vụ tấn công nào thông qua việc lợi dụng khai thác những lỗi trên.

Thông tin về những lỗi bảo mật zero-day mới trong Office được tiết lộ đúng vào ngày Microsoft phát hành bản cập nhật định kỳ tháng 4. Không những thế Microsoft còn đang phải giải quyết các hậu quả của bản cập nhật bảo mật khẩn cấp vá lỗi Windows ANI phát hành tuần trước.

Điều này đồng nghĩa với việc người dùng sẽ có một tháng không được bảo vệ và phải đối diện với nguy cơ bị tấn công bất cứ lúc nào," Raman cảnh báo.

Tin tặc hiện đã biết cách lợi dụng thông tin từ bản cập nhật định kỳ hàng tháng để tổ chức tấn công người dùng. Thông thường chả bao lâu sau khi Microsoft phát hành bản cập nhật định kỳ hàng tháng thì tin tặc sẽ tung ra mã khai thác các lỗi nhắm mục tiêu tấn công những người dùng chưa cài đặt bản vá lỗi.

Tuy nhiên, những lỗi được phát hiện lần này có thể không phải là lỗi bảo mật mới, ông Dave Marcus - Giám đốc truyền thông và nghiên cứu bảo mật của McAfee - cho biết. "Đôi khi những gì mà người ta tuyên bố là lỗi zero-day lại chỉ là những lỗi đã được vá từ lâu rồi".

Hoàng Dũng