

Microsoft phát hành bản cập nhật bảo mật Patch Tuesday

16:44 16/02/2023

Microsoft phát hành bản cập nhật bảo mật Patch Tuesday cho người dùng Windows. Bản cập nhật này vá tổng cộng 76 lỗi, bao gồm 7 lỗi nghiêm trọng và 3 lỗ hổng zero-day mà Microsoft cho biết đã bị khai thác trong thực tế.



Ảnh minh họa. (Ảnh: internet)

Trong số 3 lỗ hổng zero-day, hai lỗ hổng ảnh hưởng trực tiếp đến người dùng Windows 10 và Windows 11, cũng như hầu hết các phiên bản Windows Server từ năm 2008 trở lại đây. Lỗ hổng còn lại tác động đến người dùng Microsoft Publisher. Nếu kẻ xấu tấn công thành công, chúng có thể chiếm quyền điều khiển máy tính.

Cụ thể, lỗ hổng CVE-2023-21823 được xem là nghiêm trọng nhất. Không chỉ ảnh hưởng đến Windows 10 và 11, nó còn là một lỗ hổng RCE (thực thi mã từ xa). Điều đó đồng nghĩa kẻ tấn công có thể chạy mã trên máy tính mà không cần

đăng nhập giống như chúng là một người dùng hợp pháp. Theo Microsoft, nếu thành công, chúng có thể giành được đặc quyền hệ thống (SYSTEM privilege). Chuyên gia bảo mật Mike Walters đến từ hãng Action1 cho biết khai thác lỗ hổng này tương đối đơn giản, không cần tương tác của người dùng.

Điểm khác biệt so với các bản vá bảo mật trước đây là lần này, nó sẽ được gửi đến người dùng thông qua Microsoft Store thay vì Windows Update. Vì vậy, với những người đã vô hiệu hóa tự động cập nhật trong Microsoft Store, Microsoft sẽ không tự động gửi cập nhật.

Lỗ hổng CVE-2023-21715 nằm trong Microsoft Publisher, cho phép một tài liệu vượt qua “hàng rào bảo vệ” của Office. Kẻ tấn công sẽ lừa nạn nhân thông qua hình thức social engineering để tải về và mở tài liệu từ website, từ đó dẫn đến máy tính bị tấn công.

Nạn nhân của lỗ hổng CVE-2023-23376 tương tự CVE-2023-21823 nhưng nó không phải lỗ hổng RCE mà là lỗ hổng EOP (leo thang đặc quyền). Nếu bị khai thác thành công, quyền truy cập thông thường có thể tăng lên cấp độ hệ thống. Nó cũng không yêu cầu tương tác của người dùng.

Dù bản vá tháng 2 nhỏ hơn bản vá tháng 1, CEO HighGround.io Mark Lamb cho rằng, việc xuất hiện 3 lỗ hổng zero-day và 12 lỗi liên quan đến leo thang đặc quyền cho thấy nó vẫn là một bản cập nhật quan trọng. Richard Hollis, CEO Risk Crew, gọi đây là những bản cập nhật cần thiết, đặc biệt giữa bối cảnh người làm việc tại nhà ngày càng nhiều.

Hà Trần (t/h)