XUẤT HIỆN MÃ KHAI THÁC LỖI CHẾT NGƯỜI VISTA, XP

Hãng bảo mật Immunity hôm 17/01 đã cho phát hành mã khai thác một lỗi bảo mật chết người trong Windows mới được Microsoft cho khắc phục gần đây.

Tuy nhiên mã khai thác chưa hề được phát hành rộng rãi, chỉ có các chuyên gia bảo mật chuyên nghiệp sử dụng phần mềm kiểm tra độ bảo mật máy tính Canvas của Immunity mới được tiếp cận mã khai thác lỗi nói trên.

Dave Aitel – Giám đốc công nghệ của Immunity – cho biết mã khai thác có khả năng khiến hệ điều hành Windows treo cứng hoàn toàn đồng thời tạo điều kiện cho phép đối tượng tấn công được quyền điều khiển thực thi mã độc trên PC mắc lỗi. "Thực tế trong một số trường hợp thử nghiệm Windows PC đã cho hiển thị màn hình xanh chết chóc".

Kể từ sau khi thông tin về lỗi bảo mật nói trên được công bố giới bảo mật đã bày tỏ không ít lo ngại về khả năng bùng nổ tấn công người dùng trên diện rộng. Bởi thứ nhất đây là lỗi phát sinh trong một bộ phận cấu thành hệ điều hành Windows và được kích hoạt theo mặc định. Và thứ hai là lỗi có thể bị khai thác mà không cần bất kỳ sự can thiệp nào từ phía người dùng. Đồng nghĩa với việc lỗi này có thể bị lợi dụng để tổ chức tấn công bằng sâu máy tính tự nhân bản.

Giới bảo mật nhận định tin tặc hoàn toàn có thể theo chân các chuyên gia nghiên cứu bảo mật tiếp tục đào sâu hơn nữa vào lỗ hổng chết người này của Windows.

Lỗi bắt nguồn từ tiến trình xử lý luồng dữ liệu mạng sử dụng thủ tục IGMP (Internet Group Management Protocol) và MLD (Multicast Listener Discovery). Đây là thủ tục chuyên dụng để gửi dữ liệu sang nhiều hệ thống cùng một lúc. Rất nhiều ứng dụng như gửi nhận tin nhắn tức thời, hội thảo trực tuyến, phân phối phần mềm … đều phải sử dụng những thủ tục này. Cả Windows XP và Vista đều được xác định mắc lỗi này.

Để tấn công người dùng tin tặc cần tạo ra một gói dữ liệu độc hại gửi đến PC người dùng thông qua những thủ tục nói trên. Nếu thành công tin tặc sẽ có thể đoạt được quyền từ xa điều khiển vận hành mã độc - ở đây có thể là sâu máy tính – trên PC mắc lỗi. Con sâu này sau đó có thể tự động phát tán mạnh trong mạng nội bộ LAN.

Hiện Microsoft đã phát hành bản cập nhật sửa lỗi chết người này. Người dùng được khuyến cáo nên nhanh chóng tải về cài đặt bản cập nhật mang mã hiệu MS08-001 càng sớm càng tốt. Song song bên cạnh đó Microsoft cũng khẳng định lỗi này tương đối rất khó khai thác.