MICROSOFT LẠI "SỐC" VÌ LỖI BẢO MẬT MỚI TRONG IE

Microsoft hiện lại đang phải gấp rút tìm cách khắc phục một lỗi bảo mật "zero-day" trong Internet Explorer vừa được công bố rộng rãi có thể bị lợi dụng để tổ chức tấn công thực thi đoạn mã nguy hiểm. Microsoft đã khẳng định hiện họ đang tiến hành điều tra thêm th&

Microsoft hiện lại đang phải gấp rút tìm cách khắc phục một lỗi bảo mật "zero-day" trong Internet Explorer vừa được công bố rộng rãi có thể bị lợi dụng để tổ chức tấn công thực thi đoạn mã nguy hiểm. Microsoft đã khẳng định hiện họ đang tiến hành điều tra thêm thông tin được công bố thông qua danh sách thư điện tử "Full-disclosure mailing list". Theo kênh thông tin này thì những phiên bản mới nhất trình duyệt có thể bị "treo" khi truy cập vào một trang web có các thẻ OBJECT nguy hiểm ẩn náu. Người phát ngôn của Microsoft cho biết những điều tra ban đầu cho biết lỗi bảo mật này có thể khiến cho trình duyệt bị tự động đóng lại hoặc bị treo. "Mirosoft sẽ tiếp tục điều tra thêm những thông tin về lỗi bảo mật này nhằm đưa ra những thông tin trợ giúp cần thiết cho người sử dụng," người phát ngôn khẳng định. Michal Zalewski - người đã phát hiện ra và công bố lỗi bảo mật này – khẳng định cả phiên bản Internet Explorer 6 được vá lỗi đầy đủ chạy trên nền tảng Windows XP Service Pack 2 vẫn bị mắc lỗi này. Michal cho đây là một lỗi bảo mật khó bị khai thác nhưng vẫn cảnh báo nguy cơ về các cuộc tấn công thực thi đoạn mã từ xa. Hãng bảo mật Secunia xếp lỗi bảo mật này vào mức "cực kỳ nguy hiểm" và nhấn mạnh lỗi bảo mật này có thể bị khai thác nhằm phá huỷ bộ nhớ bằng cách lừa người sử dụng truy cập vào một trang web độc hại. "Nếu thành công trong việc khai thác lỗi bảo mật này kẻ tấn công có thể được phép thực thi các đoạn mã nhị phân," Secunia cảnh báo.

Hãng bảo mật FrSIRT của Pháp cũng cho xếp lỗi bảo mật vào mức "nghiêm trọng" và cảnh báo lỗi bảo mật có thể bị lợi dụng để tổ chức các vụ tấn công từ xa. "Lỗi bảo mật này phát sinh do lỗi phá huỷ bộ nhớ khi trình duyệt xử lý một đoạn mã HTNL nguy hiểm có chứa các thẻ 'object' cho phép kẻ tấn công ác ý từ xa chiếm toàn bộ quyền kiểm soát hệ thống mắc lỗi bằng cách lừa người sử dụng truy cập vào một trang web nguy hiểm." Các chuyên gia của Websense Security Labs khẳng định hiện vẫn chưa có bất kỳ đoạn mã có khả năng khai thác nào được phát tán nhưng cũng cảnh báo là lỗi phá hỏng trình duyệt thường có thể dẫn tới các vụ tấn công thực thi đoạn mã từ xa. "Hiện chúng tôi hiện đang tìm kiếm các trang web có khả năng khai thác lỗi bảo mật này." Microsoft đã lên tiến phê phán Zalewski vì đã cho phép công bố lỗi bảo mật này trước khi có bản vá chính thức được tung ra. Nhưng chuyên gia nghiên cứu này lại cho rằng anh hoàn toàn không có lỗi. "Tôi không hề thông báo trước cho Microsoft vì tôi muốn họ nhanh chóng khắc phục lỗi bảo mật này." Hoàng Dũng