CON TRỎ CHUỘT CÓ THỂ HẠ GỤC VISTA

Các ch

Các chuyên gia bảo mật của McAfee Avert Labs hôm qua (29/3) cho biết Windows Vista hoàn toàn có thể bị hạ gục chỉ bằng một tệp tin con chỏ chuột động. Hệ điều hành khi đó sẽ rơi vào trạng thái lặp đi lặp lai tình trạng "treo cứng - khởi động lại - treo cứng".

Không chỉ xác nhận thông tin mà các chuyên gia bảo mật của McAfee còn phát hành cả đoạn video minh chứng rõ ràng khả năng khai thác. Đây được xem là "lỗi bảo mật hài hước nhất" trong Windows Vista.

Thực tế đây là một lỗi tràn bộ nhớ đệm trong hệ điều hành. Nó không phải là một lỗi mới. Các chuyên gia bảo mật của eEye đã phát hiện được lỗi này từ tháng 1/2005.

Vào thời điểm đó Microsoft cũng đã xác nhận lỗi này tồn tại trên rất nhiều phiên bản Windows khác nhau (xem danh sách dưới). Tuy nhiên, hãng phần mềm tuyên bố Windows XP SP1 không mắc lỗi này.

Microsoft Windows 2000 Service Pack 4
Microsoft Windows XP Service Pack 2
Microsoft Windows XP 64-Bit Edition Version 2003 (Itanium)
Microsoft Windows XP Professional x64 Edition
Microsoft Windows Server 2003
Microsoft Windows Server 2003 for Itanium-based Systems
Microsoft Windows Server 2003 Service Pack 1
Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
Microsoft Windows Server 2003 x64 Edition
Microsoft Windows Vista

Cho đến thời điểm hiện tại số lượng các vụ tấn công bằng cách khai thác lỗi bảo mật nói trên còn tương đối hạn chế.

Gần đây nhất Avert Labs phát hiện được một mã khai thác cũng sử dụng tệp tin ".ani" để tấn công hàng loạt phiên bản Windows - gồm Windows 2000 SP4, Windows Server 2003 (phiên bản đầu tiên đến phiên bản SP1), Windows XP SP2 và Windows Vista.

Avert Labs xác nhận cho đến nay chưa có mã khai thác kiểu như thế tấn công được Windows XP SP1. Microsoft cũng thừa nhận XP SP2 mắc lỗi. Điều này đồng nghĩa với việc Microsoft khắc phục được lỗi trong XP SP1 rồi lại bỏ ngỏ nó trong các phiên bản hệ điều hành sau đó.

Nội dung đoạn video của Avert Labs cho thấy Vista trong khi cố gắng tải một tệp tin con chỏ chuột động thì hệ thống báo phát sinh lỗi và khởi động lại. Tình trạng này tiếp tục lặp lại liên tục ngay cả khi hệ thống đã khởi động lại thành công. Người dùng không thể dùng hệ điều hành được nữa.

Hệ thống xử lý tín hiệu con chỏ chuột đầu vào của Windows được thiết kế với khả năng chống lại các sự cố bất ngờ. Chính vì thế mà khi hệ thống rơi vào tình trạng treo cứng nhưng người dùng vẫn có thể di chuyển được chuột. Nhưng thiết kế tính năng như thế đôi khi cũng khiến Windows Explorer treo cứng và rơi vào trạng thái liên tục phải khởi động lại.

McAfee cho biết hiện mã khai thác này đã được phát tán rộng rãi trên mạng Internet. Microsoft đã lên tiếng khuyến cáo người dùng không nên mở các tệp tin đính kèm theo các email không rõ nguồn gốc.

Hoàng Dũng