LỖI CARD ĐỒ HOẠ ATI GIÚP MÃ ĐỘC ĐỘT NHẬP VISTA

Một lỗ

Một lỗ hổng bảo mật nghiêm trọng trong trình điều khiển card đồ hoạ ATI có thể bị mã độc lợi dụng để giúp chúng qua mặt các tường rào bảo mật và đột nhập thẳng vào nhân hệ điều hành Windows Vista.

Nhà phát triển Alex Ionescu là người có công phát hiện lỗi bảo mật card đồ hoạ ATI. Và chỉ một vài giờ sau khi phát hiện lỗi Ionescu đã cho ra ngay một công cụ khai thác lỗi Purple Pill có khả năng tự động tải hoặc không tải trình điều khiển trên Vista.

Mã độc có thể được chèn trực tiếp vào đây. Purple Pill qua mặt cơ chết chống rootkit của Vista bằng cách vô hiệu hoá khả năng kiểm tra trình điều khiển thiết bị của cơ chế này.

Purple Pill đột nhập vào Vista bằng cách tự ẩn mình trên chứng thực bảo mật (security certificate) tích hợp sẵn trong các phần mềm trình điều khiển thiết bị.

“Cái mà ATI cần làm hiện nay là phải có được một chứng thực bảo mật mới, khắc phục lỗ hổng trong trình điều khiển, và phát hành nó thông qua tính năng Windows Update của Microsoft,” ông Ollie Whitehouse - một chuyên gia nghiên cứu bảo mật của Symantec - nhận định.

“Tôi cho rằng lỗi trên bắt nguồn từ việc thiết kế và phát triển trình điều khiển thiết bị của ATI.”

Microsoft và ATI hiện đang tích cực hợp tác nhằm tìm giải pháp bít lỗ hổng bảo mật “chết người” nói trên sớm chừng nào hay chừng đó.

Hoàng Dũng