HIỂM HOẠ BẢO MẬT TỪ... MÁY IN XEROX

Hôm qua (4/8), một lỗi bảo mật nghiêm trọng trong máy in đa chức năng WorkCenter của Xerox có thể bị lợi dụng để làm công cụ tấn công đã được tiết lộ tại Black Hat. Bằng các lợi dụng một lỗi cấu hình trong giao diện web của loại máy in nói trên, chuyên

Hôm qua (4/8), một lỗi bảo mật nghiêm trọng trong máy in đa chức năng WorkCenter của Xerox có thể bị lợi dụng để làm công cụ tấn công đã được tiết lộ tại Black Hat. Bằng các lợi dụng một lỗi cấu hình trong giao diện web của loại máy in nói trên, chuyên gia nghiên cứu bảo mật Brendan O'Connor có thể chạy các phần mềm không được phép trên thiết bị, theo dõi, bắt các gói tin trong mạng và thu thập được các thông tin nhạy cảm đã được in qua máy in WorkCenter. Chuyên gia O'Connor đã cho công bố chi tiết về cách thức tấn công bằng các lợi dụng lỗi bảo mật trong máy in WorkCenter tại Hội nghị Black Hat năm nay.

Máy in Xerox WorkCenter

Trong khi đó, nhà phát triển sản phẩm Xerox đang phải gấp rút phát triển bản cập nhật bảo mật nhằm khắc phục vấn đề nói trên. Hiểm hoạ tiềm tàng cho doanh nghiệp "Hãy thử nghĩ về các dữ liệu nhạy cảm được in qua máy in WorkCenter," chuyên gia O'Connor nói. "Người dùng chỉ biết in và tin tưởng vào những thiết bị như thế này. Người dùng chưa biết về những mối đe doạ tiềm tàng nằm trong đó." O'Connor khẳng định ông muốn sử dụng "trường hợp Xerox" để cảnh báo mọi người về những mối đe doạ bảo mật tiềm tàng trong các thiết bị nhúng nhiều tính năng mạnh mẽ đang ngày càng được sử dụng rộng rãi, đặc biệt trong môi trường doanh nghiệp. "Tôi cho rằng vấn đề này vẫn chưa nhận được sự quan tâm thích đáng," O'Connor - một chuyên gia bảo mật của một công ty tài chính nhỏ tại Mỹ - khẳng định. Sản phẩm nào mắc lỗi? Tháng 2 vừa qua, Xerox đã phát hành một bản vá lỗi bảo mật cho dòng sản phẩm WorkCenter và WorkCenter Pro 200 Series được bán ra trong khoảng thời gian từ tháng 10/2005 đến tháng 6/2006, Armon Rahgozar - Giám đốc công nghệ và giải pháp văn phòng đối tác Xerox - cho biết. Tuy nhiên, bản vá lỗi đó vẫn chưa hoàn toàn khắc phục được các lỗi bảo mật, O'Connor khẳng định. "Bản thân nơi công ty tôi đang làm việc cũng vẫn rất dễ bị tấn công thông qua những lỗi bảo mật đó". Rahgozar cho biết Xerox đang khẩn trương nghiên cứu tìm giải pháp khắc phục lỗi bảo mật nói trên. Khách hàng có thể tải về bản vá lỗi thông qua trang web của Xerox hoặc chờ đợi các kỹ sư của hãng đến cài đặt khắc phục mọi vấn đề trong đợt dịch vụ khách hàng sắp tới. Bên cạnh đó, Xerox cũng đang phát triển một hệ thống tự động cập nhật tương tự như hệ thống trong Windows của Microsoft cho các sản phẩm của hãng, Rahgozar nói. "Chúng tôi muốn đi theo mô hình mà Microsoft đã phải mất khá nhiều mới học được." Hoàng Dũng