LỖI FLASH ĐE DOẠ HÀNG TRĂM NGHÌN HỆ THỐNG MẠNG

Hai ch

Hai chuyên gia nghiên cứu bảo mật cuối tuần qua đã cho phát hành mã khai thác lỗ hổng bảo mật nghiêm trọng trong hai công nghệ được sử dụng rộng rãi. Lỗi này hoàn toàn có thể bị lợi dụng để kiểm soát toàn bộ tiến trình duyệt web của người dùng.

Adrian Pastor và Petko Petkov cho biết hai công nghệ mắc lỗi ở đây là thủ tục Universal Plug and Play (UPnP) thường được sử dụng trong các hệ điều hành và Adobe Flash.

Chỉ cần lừa được người dùng mở xem một tệp tin Flash độc hại tin tặc sẽ có thể sử dụng thủ tục UPnP để thay đổi máy chủ tên miền DNS gốc (DNS Primary Server) định sẵn trên các bộ định tuyến mạng (router). Qua đó cho phép chúng chuyển hướng truy cập của người dùng trong mạng sang một website độc hại thay vì website mà họ muốn truy cập vào.

"Thay đổi máy chủ tên miền DNS gốc hành động được xem là nguy hiểm nhất," hai chuyên gia bảo mật chia sẻ chung một quan điểm. "Hành động này cho phép tin tặc có thể chiếm được toàn bộ quyền điều khiển hệ thống mạng mắc lỗi biến nó thành một mạng zombie giúp chúng thực hiện các hành vi tấn công khác".

Pastor và Petkov nhận định có tới 99% bộ định tuyến mạng gia đình hiện đang phải đối diện với nguy cơ bị tấn công bởi hầu hết các router này đều có hỗ trợ công nghệ UPnP. Thậm chí một số thiết bị cũng có hỗ trợ UPnP khác như máy tin, hệ thống giải trí số hay camera kỹ thuật số cũng có thể bị tấn công bằng phương thức này.

Nguy cơ đa nền tảng

Lỗi bảo mật được phát hiện bởi Adrian Pastor và Petko Petkov được đánh giá là cực kỳ nguy hiểm bởi nó có thể mở đường cho các vụ tấn công đa nền tảng. Bất kỳ hệ điều hành nào có hỗ trợ công nghệ Flash đều có thể bị tấn công. Bởi thực chất lỗ hổng bị khai thác để tấn công là một tính năng của Flash và UPnP chứ không hẳn là một lỗi bảo mật. Thêm một vấn đề nữa là những lỗi này cũng không dễ dàng được khắc phục bởi Adobe hoặc nhà sản xuất router. Lỗi nằm chính trong bản chất của công nghệ.

Người dùng có thể hạn chế nguy cơ bị tấn công bằng cách vô hiệu hoá tính năng sử dụng thủ tục UPnP trên các router. Tuy nhiên, điều này sẽ gây ảnh hưởng đến không ít các ứng dụng được

dùng rất phổ biến như ứng dụng gửi nhận tin nhắn tức thời, games hoặc Skype.

Chuyên gia nghiên cứu bảo mật Aviv Raff cho biết Adobe cũng có thể thay đổi công nghệ Flash để giúp hạn chế bớt nguy cơ bị tấn công. Song tin tặc cũng hoàn toàn có thể sử dụng kỹ thuật tấn công khác để lợi dụng tối đa lỗi bảo mật.

"Đây là một lỗ hổng bảo mật cực kỳ nghiêm trọng. Tôi khuyến cáo người dùng nên nhanh chóng vô hiệu hoá các thiết bị sử dụng UPnP. Các nhà sản xuất thiết bị cũng không nên mặc định kích hoạt tính năng UPnP trên thiết bị của mình khi tung ra thị trường".

Hiện vẫn chưa có dấu hiệu nào cho thấy tin tặc đã phát hiện và bắt đầu lợi dụng lỗi bảo mật nghiêm trọng nói trên để tấn công người dùng.