MICROSOFT BẮT TAY VÁ LỖ HỔNG WEB PROXY 8-NĂM-TUỔI

Micros

Microsoft bắt tay vào việc vá một lỗ hổng đã tồn tại cách đây 8 trong Windows, lỗ hổng này "giúp" các hacker khai thác được giao thức cấu hình tự động của Web proxy và quản lý các máy tính chỉ thông qua một cuộc tấn công.

Lỗ hổng này được phát hiện vào năm 1999 và các chuyên gia cho rằng nó có lẽ không bao giờ được chính thức vá lại.

Lỗ hổng này ảnh hưởng tới tất cả cá phiên bản Windows trong đó bao gồm cả Vista, nhưng các máy tính ở tại Mỹ thì lại không bị ảnh hưởng. Microsoft đã thông tin bản vá lỗi cho lỗ hổng "8 năm tuổi" này nhằm bảo vệ các máy tính sử dụng tên miền ".com". Tuy nhiên, bản vá này không làm việc đối với các máy sử dụng têm miền hệt thống quốc gia như .nz (New Zealand) hay .uk (United Kingdom).

WPAD là phương thức được sử dụng bởi các trình duyệt web nhằm xác định file cấu hình proxy – file wpad.dat – dùng để cấu hình các thiết lập proxy cho trình duyệt web. Vai trò của lỗi này là cho phép tìm kiếm file cấu hình đã bỏ đi sự an toàn của mạng nội bộ, qua đó mở đường cho hacker tấn công thực hiện yêu cầu và mở một file cấu hình trình duyệt, sau đó thực hiện việc ngăn chặn và chỉnh sửa lưu lượng web của người dùng.

Tính năng WPAD của Windows được thiết kế để các quản trị viên không cần phải cấu hình các thiết lập proxy trình duyệt cho từng máy tính đơn lẻ một cách thủ công. Tất cả được cấu hình WPAD tự động mà không cần sự theo dõi của người dùng.

Tuần trước, Beau Butler – người đã biết đến với cái tên Oddy và danh hiệu "hacker chính nghĩa" – đã trình bày những khám phá thêm về lỗ hổng WPAD tại hội nghị Kiwicon hàng năm tổ chức tại NewZealand vừa rồi. Butler nói với những người tham dự hội nghị và trên website The Age của Australia rằng anh đã tìm thấy 160,000 máy tính ở New Zealand sử dụng tên miền .nz gặp phải lỗ hổng WPAD. The Age có nói Microsoft đã yêu cầu họ không công bố chi tiết mối đe doạ này tránh việc những kẻ tội phạm mạng sử dụng chúng để điều khiển các trạm làm việc. Microsoft xác nhận rằng đây là một vấn đề nghiêm trọng.

Tuy nhiên một vài chi tiết về lỗi này vẫn có thể tìm thấy bằng cách thực hiện một truy vấn đơn giản trên chính trang tìm kiếm Live Search của Microsoft. Ngoài ra, Microsoft còn có mô tả cách WPAD

làm việc trên trang Knowledge Base.

Trong bản tóm tắt tại hội nghị Kiwicon có nói Oddy (Butler) còn "giải thích tất cả phương thức trong các mạng có thể được cấu hình để tạo lổ hổng WPAD". Theo thông tin từ website của Microsoft "WPAD cho phép các dịch vụ xác định một máy chủ proxy hoạt động bằng cách truy vấn một tuỳ chọn DHCP (giao thức cấu hình máy chủ động) hoặc bằng cách xác định một bản ghi DNS cụ thể"

Chuyên gia lưu trữ web Duane Wessels - người đã giúp phát triển Squid, một máy chủ lưu trữ proxy có độ thực thi cao – đã có một website giải thích lỗ hổng cho những người dùng. "Về cơ bản nó làm việc như sau: Khi trình duyệt được mở, nó sẽ đưa ra một tìm kiếm địa chỉ DNS cho 'wpad.foo.com' với 'foo.com' là tên miền của máy tính. Do lỗi của Microsoft, một vài trình duyệt sẽ tìm kiếm 'wpad.com', đây chính là máy chủ của tôi", ông đã viết như vậy trên website của mình.

Trên thực tế việc tìm kiếm DNS chỉ xảy ra khi DHCP không bị rối loạn bởi file wpad.dat. DNS là tuỳ chọn tiếp theo và việc tìm kiếm 'wpad.com' xảy ra như hệ luỵ của WPAD. Hệ đẳng cấp DNS sẽ tìm kiếm địa chỉ của file cấu hình proxy wpad.dat. WPAD điển hình có thể ước chừng tìm được chính xác ngay trong mạng nội bộ của công ty, nhưng đối với các tên miền cấp quốc gia quá trình tìm sẽ bị chệch đi và nó sẽ tự động tìm kiếm ra bên ngoài mạng của tổ chức.

Không quan tâm tới các vị trí tìm kiếm mở rộng ra bao xa, một khi đã xác định được file wpad.dat thành công, trình duyệt sẽ tạo một kết nối và lấy file đó về cấu hình cho trình duyệt. Nếu một hacker thành công trong việc đặt file wpad.dat của hắn vào cấu hình trình duyệt, kẻ tấn công có thể trỏ trình duyệt về các proxy của hắn, ngăn chặn và chỉnh sửa tất cả các lưu lượng HTTP ra vào trình duyệt.