LỖI BẢO MẬT ZERO-DAY TRONG WINDOWS

Lỗi bả

Lỗi bảo mật mới nhất thuộc dạng “zero-day” trong Windows XP SP2 vừa được công bố mã khai thác trên các website hacker có thể bị khai thác tấn công từ chối dịch vụ đối với người dùng đang sử dụng phiên bản Windows XP SP2.

Các kẻ tấn công khai thác tấn công từ chối dịch vụ (DoS) nhằm vào mục tiêu là tập tin thư viện động “ipnathlp.dll”, được sử dụng cho dịch vụ tường lửa Windows Firewall / Internet Connection Sharing (ICS).

Tập tin thư viện động ipnathlp.dll (NAT Helper Components) kết nối đến các hệ thống Windows XP với Internet Connection Sharing. Một tài khoản người dùng trong cùng mạng chia sẻ có thể gởi một truy vấn DNS “thủ công” đặc biệt đến hệ thống mục tiêu để “ipnathlp.dll” xử lý và dẫn đến việc tấn công từ chối dịch vụ. Khi hệ thống đã bị tấn công, sẽ xuất hiện tin nhắn: “Generic Host Process for Win32 Services has encountered a problem and needs to close. We are sorry for the inconvenience”.

Lỗi hiện tại đe dọa đến toàn bộ hệ thống đang sử dụng Windows XP SP2, không ảnh hưởng tới Windows Server 2003. Giải pháp hiện thời là sử dụng một cách thức khác để chia sẻ kết nối Internet, người dung có thể tham khảo thêm một vài giải pháp tại đây.

TUYẾT PHẤN