MICROSOFT CẢNH BÁO VỀ LỖ HỔNG MỚI TRONG WINDOWS

Cuối ngày thứ 4 vừa qua, Microsoft đã cảnh báo người sử dụng về một đoạn mã đã được kiểm chứng tính nguy hiểm có thể từ xa thác lỗ hổng bảo mật trong các hệ thống chạy hệ điều Windows 2000 đang lan tràn trên mạng. Cũng theo Microsoft không chỉ riêng các h

Cuối ngày thứ 4 vừa qua, Microsoft đã cảnh báo người sử dụng về một đoạn mã đã được kiểm chứng tính nguy hiểm có thể từ xa thác lỗ hổng bảo mật trong các hệ thống chạy hệ điều Windows 2000 đang lan tràn trên mạng. Cũng theo Microsoft không chỉ riêng các hệ thống chạy Windows 2000 mới chịu ảnh hưởng của lỗ hổng bảo mật mới này mà một số hệ thống chạy Windows XP SP1 cũng bị. Hiện chưa có bất kỳ miếng vá nào được ban hành. Trong bản tin bảo mật mới nhất của mình, Microsoft cũng mới chỉ đưa ra một số thông tin chi tiết về lỗ hổng bảo mật mới này. Theo nhà phát triển cho biết lỗ hổng bảo mật mới này phát sinh trong thành phần RPC (Remote Procedure Call) của hệ điều hành Windows. Tin tặc hoàn toàn có thể lợi dụng lỗ hổng này để khởi động các cuộc tấn công từ chối dịch vụ phá hỏng hệ thống máy tính của người sử dụng. “Trên một hệ thống chạy Windows XP Service Pack 1, một kẻ tấn công mưu mô cần phải có một tài khoản đăng nhập chuẩn mới có thể khai thác được lỗ hổng bảo mật này,” Microsoft cho biết trong bản tin bảo mật. Nhưng đối với các hệ thống chạy Windows 2000 thì tin tặc lại không cần điều đó, có thể từ xa điều khiển cuộc tấn công. Những phiên bản hệ điều hành cũ như Windows 2000 trong khoảng thời gian trở lại đây đã trở thành mục tiêu tấn công trong của tin tặc nhắm vào các lỗ hổng bảo mật khá nghiêm trọng trong đó phải kể đến sự bùng nổ của Zotob. Windows XP SP2, Windows Server 2003, và Windows Server 2003 SP1 không bị ảnh hưởng bởi lỗ hổng bảo mật này. Tuy nhiên, theo những gì mà Microsoft đã ghi nhận được thì cho đến nay chưa có bất kỳ một cuộc tấn công nào nhắm vào việc khai thác lỗ hổng bảo mật lần này nhưng dù sao thì vấn đề vẫn đang được điều tra làm rõ thêm. Có thể trong thời gian sớm nhất hãng sẽ cho ban hành bản vá lỗi bảo mật này. Microsoft cũng mới chỉ đưa ra một số khuyến cáo chung chung nhằm hạn chế việc người sử dụng có thể bị khai thác lỗ hổng bảo mật này. “Tường lửa là biện pháp tốt nhất. Người sử dụng nên sử dụng những thiết lập mặc định của tường lửa là cũng đủ để bảo vệ minh khỏi các cuộc tấn công.”