PHỔ BIẾN ĐOẠN MÃ NGUY HIỂM KHAI THÁC LỖI WINDOWS

Cuối tuần qua một đoạn mã nguy hiểm nhằm khai thác một lỗ hổng bảo mật có khả năng phá hỏng các hệ thống chạy hệ điều hành Windows đã được cho công bố rộng rãi trên Internet. Đoạn mã khai thác nguy hiểm mới này nhắm mục tiêu khai thác một lỗi bảo m

Cuối tuần qua một đoạn mã nguy hiểm nhằm khai thác một lỗ hổng bảo mật có khả năng phá hỏng các hệ thống chạy hệ điều hành Windows đã được cho công bố rộng rãi trên Internet. Đoạn mã khai thác nguy hiểm mới này nhắm mục tiêu khai thác một lỗi bảo mật trong hệ điều hành Windows mà Microsoft xếp vào mức "cực kì nguy hiểm". Lỗi này phát sinh trong một bộ phận của hệ điều hành có tên gọi là Microsoft Distributed Transaction Coordinator (MSDTC). Microsoft đã cho ban hành bản vá lỗi bảo mật này cùng với bản tin bảo mật tháng 10 - miếng vá MS05-051. Theo một đại diện của Microsoft cho biết: Những điều tra ban đầu về đoạn mã này cho thấy đoạn mã này hoàn toàn có đủ khả năng khai thác thành công lỗ hổng bảo mật trong hệ điều hành Windows và có thể dẫn tới một cuộc tấn công từ chối dịch vụ. Đại diện của Microsoft cũng khẳng định, đoạn mã này không thể tấn công bằng cách thực thi đoạn mã từ xa. Tấn công bằng việc thự thi các đoạn mã nguy hiểm từ xa thường đồng nghĩa với việc tin tặc có thể đoạt quyền kiểm soát toàn bộ PC của người sử dụng trong khi đó tấn công từ chối dịch vụ chỉ gây ra hỏng hóc cho hệ thống. Cũng theo Microsoft thì nếu người sử dụng đã cài đặt bản vá lỗi MS05-051 thì hệ thống của họ được bảo đảm "miễn dịch" với đoạn mã khai thác nguy hiểm mới này. Đây không phải là đoạn mã nguy hiểm khai thác lỗi trong MSDTC đầu tiên được công bố nhưng lại là đoạn mã nguy hiểm đầu tiên khai thác lỗi bảo mật này được công bố rộng rãi trên Internet. Đoạn mã đầu tiên được hãng bảo mật Immunity lập trình nên phục vụ cho việc kiểm tra các sản phẩm. Khi Microsoft ban hành bản vá lỗi này các chuyên gia đã nhanh chóng cảnh báo rằng lỗ hổng bảo mật trong thành phần MSDTC có thể sẽ gây ra một cuộc tấn công quy mô tương tự như những gì mà sâu máy tính Zotob đã làm trong tháng 8. Tuy nhiên những cuộc tấn công như thế này hiện chưa xuất hiện. Nhưng việc xuất hiện của đoạn mã nguy hiểm này có thể là dấu hiệu đầu tiên cho thấy những cuộc tấn công đang đến. Microsoft lại cho rằng hãng này không lo ngại về những cuộc tấn công có sử dụng đoạn mã nguy hiểm mới được công bố này. Nhưng hãng cũng khuyến cáo người sử dụng nên nhanh chóng cài đặt các bản vá lỗi mới nhất có thể. HVD