NHÂN LINUX "DÍNH" LỖI CHẾT NGƯỜI

Các ch

Các chuyên gia bảo mật mới đây đã phát hiện 3 lỗi bảo cực kỳ nguy hiểm trong nhân một số phiên bản hệ điều hành mã nguồn mở Linux được sử dụng tương đối phổ biến như Ubuntu, Turbolinux, SuSE, Red Hat, Mandriva, Debian...

Hãng bảo mật SecurityFocus cho biết những lỗi bảo mật này có thể bị tin tặc lợi dụng để đọc ghi dữ liệu lên phân vùng bộ nhớ nhân hệ điều hành hoặc đoạt quyền truy cập tới các tài nguyên hệ thống máy chủ.

Các lỗi bảo trên - giới bảo mật khuyến cáo - còn có thể bị lợi dụng để tấn từ chối dịch vụ, ăn cắp thông tin dữ liệu hoặc đoạt quyền truy cập cấp độ ROOT tới hệ thống sử dụng phiên bản hệ điều hành mắc lỗi.

Phiên bản nhân hệ điều hành Linux được xác nhận mắc lỗi là phiên bản 2.6.24.1. Đây là phiên bản nhân được sử dụng tương đối phổ biến. Hầu hết các phiên bản Linux hiện có trên thị trường đều sử dụng phiên bản nhân này.

Hãng bảo mật Secunia cho biết nguyên nhân phát sinh lỗi là từ 3 hàm (functions) trực thuộc hệ thống "system call fs/splice.c". "Có thể nói lỗi bắt đầu phát sinh từ phiên bản nhân 2.6.23. Đây là thời điểm hàm gọi hệ thống được mở rộng hơn. Ngoài các tiện ích bổ sung, việc mở rộng cũng mang lại các lỗi bảo mật cực kỳ nguy hiểm".

Mã khai thác những lỗi bảo mật nhân Linux nói trên hiện đã được công bố rộng rãi thông qua webiste Milw0rm.com. Riêng Core Security Technology còn phát triển hẳn một phiên bản công cụ khai thác lỗi thương mại dành riêng cho việc thử nghiệm những lỗi nhân Linux trên đây.

Các chuyên gia bảo mật khuyến cáo các nhà quản trị hệ thống sử dụng Linux nên nhanh chóng nâng cấp nhân hệ điều hành càng sớm càng tốt.