SYMANTEC VÁ LỖ HỔNG TRONG ỨNG DỤNG BACKUP EXEC

Cuối tuần qua, Symantec đã công bố chi tiết một lỗ hổng trong giải pháp lưu trữ Backup Exec của hãng này, từng cho phép kẻ tấn công từ xa chiếm quyền điều khiển toàn bộ hệ thống, và truy nhập trái phép và những dư liệu nhạy cảm lưu trữ trên mạng doanh nghiệp. Sy

Cuối tuần qua, Symantec đã công bố chi tiết một lỗ hổng trong giải pháp lưu trữ Backup Exec của hãng này, từng cho phép kẻ tấn công từ xa chiếm quyền điều khiển toàn bộ hệ thống, và truy nhập trái phép và những dư liệu nhạy cảm lưu trữ trên mạng doanh nghiệp. Symantec xác nhận lỗ hổng trên ảnh hưởng tới phiên bản Symantec Backup Exec 9.1 và 9.2 dành cho NetWare Servers và Windows Servers. Symantec đã ban hành bản sửa lỗi dành cho lỗ hổng trong NetWare, và đang nghiên cứu các báo cáo cho rằng lỗ hổng còn ảnh hưởng tới cả ứng dụng Backup Exec dành cho Windows Servers, Backup Exec Continuous Protection Server (CPS) Remote Agent và Backup Exec Remote Agents. Lỗ hổng trên tác động tới giao thức gọi từ xa (RPC) của ứng dụng Backup Exec, có thể cho phép kẻ tấn công từ xa gửi mã độc hại tới ứng dụng và chiếm quyền điều khiển hệ thống đích. Thậm chí ngay cả khi những tác vụ này không thể thực hiện, lỗ hổng RPC vẫn có thể gây ra một vụ tấn công DoS. Tháng 8/2005, Symantec cũng cho vá một lỗ hổng trong ứng dụng Backup Exec dành cho Windows và NetWare, từng cho phép tin tặc giả mạo mật khẩu trong quá trình định danh giữa máy chủ và tác nhân (agent), trao quyền truy cập tới các tệp tin lưu trữ trên máy chủ.