US-CERT: HACKER ĐANG KHAI THÁC LỖ HỔNG CSDL ACCESS

Cảnh b

Cảnh báo mới nhất của Nhóm phản ứng máy tính khẩn cấp Mỹ (US-CERT) cho biết tội phạm mạng đang khai thác một lỗ hổng trong cơ sở dữ liệu (CSDL) Microsoft Office Access để cài đặt phần mềm trái phép trên máy tính nạn nhân.

Theo cảnh báo ngắn gọn của US-CERT đưa ra ngày 12/12, tổ chức này cho biết đã phát hiện các hành vi gửi file Microsoft Access Database (.mdb) được thiết kế đặc biệt cho nạn nhân của tin tặc.

Các file .mbd được viết cho mục đích thực thi lệnh trên máy tính, chính vì thế theo khuyến cáo của Microsoft, người dùng không chạy các file này từ những nguồn không an toàn.

Symantec cho biết, thông thường các công ty luôn chặn file .mbd nhưng các nhóm tội phạm có thể hướng cuộc tấn công tới những mục tiêu cụ thể. Tuy nhiên, cho thấy thời điểm này, bản thân Symantec vẫn chưa nhận được báo cáo về trường hợp khai thác file .mdb để tấn công.

Mặc dù US-CERT không nói rõ tin tặc đang khai thác lỗ hổng nào, nhưng theo dự đoán của Symantec thì đó có thể là lỗi tràn bộ đệm mới được phát hiện gần đây trong động cơ Microsoft Jet DataBase dùng để xử lý các file Access.

Văn Hân