CHECK POINT CÓ THỂ "VÁ" ĐIỂM YẾU ZERO-DAY MỚI NHẤT CỦA MICROSOFT

Check

Check Point® Software Technologies Ltd vừa thông báo rằng các sản phẩm tường lửa và chống xâm nhập của Check Point như VPN-1, VPN1-Power, VSX, UTM-1, InterSpect và IPS-1 có khả năng bảo vệ hệ thống trước một lỗi tràn bộ đệm mới và nghiêm trọng thông qua dịch vụ Check Point SmartDenfense.

Đây là điểm yếu mới (mang mã CVE-2007-0038) được công bố trong bản tin về bảo mật MS07-017 của Microsoft. Điểm yếu này tồn tại trong các hệ điều hành Windows 2000, XP, 2003 và Vista. Nó cho phép kẻ tấn công thực hiện các tấn công tràn bộ nhớ đệm, chèn thêm và thực thi các đoạn mã trên máy trạm, máy chủ với quyền cao nhất. Kẻ tấn công khởi tạo các cuộc tấn công bằng cách đánh lừa người sử dụng thực hiện một hành động nào đó như bấm vào link trên thư điện tử.

Thậm chí trước khi có thông tin về các lỗ hổng gần đây nhất của Microsoft thì các khách hàng của Check Point đã sẵn sàng được bảo vệ bởi tính năng tường lửa và phòng chống xâm nhập có trong các sản phẩm VPN-1 UTM, VPN-1 Power, VSX, UTM-1, InterSpect và IPS-1.

"Phòng chống và bảo vệ hệ thống trước lỗi "zero day" là yêu cầu cơ bản để xây dựng một hệ thống mạng có hiệu quả cao". Oded Gonda phó giám đốc an ninh mạng của Check Point cho biết. Với việc áp dụng phương pháp tìm kiếm và phân tích để nhận diện các loại mã độc và đặc trưng tấn công, các sản phẩm tường lửa và phòng chống xâm nhập của Check Point đều cung cấp khả năng phòng thủ có thể chống lại các tấn công mới.

Để biết thêm thông tin về điểm yếu, bạn có thể vào website: http://www.checkpoint.com/defense/advisories/public/2007/cpai-04-Apr.html

Hoàng Chi