LỖI MẠNG VPN ĐE DỌA BẢO MẬT DỮ LIỆU DIỆN RỘNG

Một lỗ hổng xuất hiện trong giao thức bảo mật Internet then chốt của hầu hết các sản phẩm mạng riêng ảo (VPN) khiến hệ thống doanh nghiệp có nguy cơ gặp phải nhiều kiểu tấn công khác nhau, kể cả DoS.

Các chuyên gia nghiên cứu tại đại học Oulu (Phần Lan) cho biết họ đã phát hiện ra lỗi trong công nghệ bảo mật mạng và giao thức quản lý khóa (ISAKMP), được sử dụng trong mạng ảo IPsec và sản phẩm tường lửa của nhiều công ty như Juniper Networks và Cisco. "Những lỗi này có thể tạo điều kiện cho tội phạm mạng tấn công từ chối dịch vụ, tận dụng lỗ hổng trong chuỗi ký tự định dạng, làm tràn bộ đệm và giảm tốc độ truyền dữ liệu qua Internet. Trong một số trường hợp nhất định, kẻ tấn công còn có khả năng xử lý mã và khống chế thiết bị từ xa", Trung tâm bảo mật cơ sở hạ tầng quốc gia (NISCC) của Anh khuyến cáo. Cisco cho biết lỗi bảo mật có thể khiến một số thiết bị của hãng phải liên tục xác lập lại, do đó có thể tạo ra tấn công từ chối dịch vụ. Công ty này đã phát hành bản nâng cấp phần mềm miễn phí và hướng dẫn tại đây. Danh sách những sản phẩm bị ảnh hưởng bao gồm Cisco IOS, Cisco PIX Firewall, Cisco Firewall Services Module, Cisco VPN 3000 Serie và MDS Series SanOS. Những sản phẩm bị ảnh hưởng của Juniper bao gồm tất cả các thiết bị định tuyến thuộc dòng M, T, J, E, và hầu hết các phiên bản của phần mềm bảo mật Junos và JunoSe. Openswan Project, phần mềm IPsec xuất hiện trong nhiều sản phẩm Linux, cũng bị nguy cơ. Tổ chức hậu thuẫn chương trình này đã phát hành bản update Openswan 2.4.2 ngay khi nhận được thông báo. IBM và Microsoft tuyên bố hệ thống của họ vẫn an toàn.T.N. (CNet)