PHẦN MỀM BẢO MẬT SẮP BIẾN THÀNH MỤC TIÊU CHÍNH CỦA HACKER

F-Secure vừa phải phát hành gấp bản vá những lỗ hổng cho phép thực thi đa mã trong gói phần mềm của họ. Điều này một lần nữa khiến người ta lo ngại rằng việc các ứng dụng an ninh trở thành đối tượng lợi dụng của hacker không còn là lý thuyết. Hãng sản x

F-Secure vừa phải phát hành gấp bản vá những lỗ hổng cho phép thực thi đa mã trong gói phần mềm của họ. Điều này một lần nữa khiến người ta lo ngại rằng việc các ứng dụng an ninh trở thành đối tượng lợi dụng của hacker không còn là lý thuyết. Hãng sản xuất công cụ diệt virus tại Phần Lan này xếp phiên bản cập nhật ở mức "rất quan trọng" do lỗ hổng hỗ trợ kẻ xấu vượt qua vòng kiểm duyệt để tiếp cận và khống chế hệ thống. Sự kiện này xuất hiện chỉ vài tuần sau khi công ty đối thủ Symantec (Mỹ) công khai thừa nhận lỗi tràn bộ đệm "nghiêm trọng" trong AntiVirus Library của họ có khả năng bị lợi dụng để xử lý mã nguy hiểm. Thierry Zoller, một chuyên gia nghiên cứu độc lập tại Luxembourg, khi xem xét vấn đề của F-Secure đã phát hiện ra rằng nhiều công ty bảo mật cũng đang phát hành sản phẩm với lỗi tương tự. "F-Secure là đơn vị đầu tiên công bố lỗi", Zoller nói. "Trong khi đó, một số hãng khác đã âm thầm cập nhật hoặc đưa ra cảnh báo thay đổi nhỏ nhằm che dấu thực tế rằng các cơ chế diệt virus đang gặp trục trặc". Zoller từ chối tiết lộ tên những công ty này. 12 tháng qua, một số tên tuổi lớn trong ngành bảo mật đã phải tung ra nhiều bản cập nhật vá lỗi. Giới quan sát cho rằng ngày hacker khai thác sản phẩm diệt virus để tấn công hệ thống đang đến rất gần. "Điều ngạc nhiên là chúng ta chưa từng chứng kiến một trường hợp nào như thế", Johannes Ullrich, Giám đốc kỹ thuật tại trung tâm bảo mật SANS (Mỹ), nói. "Phần mềm bảo mật là chương trình đầu tiên đối diện với mã nguy hiểm và tồn tại trên gần như mọi desktop, do đó nếu có vấn đề, chúng thực sự là một mục tiêu hoàn hảo". Trong danh sách 20 lỗ hổng năm 2005, SANS đề cập đến sự gia tăng số lỗi trong các ứng dụng máy khách, kể cả phần mềm diệt virus và sao lưu dự phòng (backup). Alex Wheeler, một chuyên gia nghiên cứu độc lập, cũng thống kê các lỗi có thể giúp hacker làm tràn bộ đệm từ xa trong chương trình của Symantec, Panda, Kaspersky Lab và Sophos. "Một ngày không xa, ai đó sẽ thực hiện một cuộc khai thác quy mô lớn, gây lỗi tràn bộ đệm nghiêm trọng và có sức tàn phá ngang với bất cứ cuộc tấn công tự động bằng sâu nào", Marc Maiffret, Giám đốc bộ phận khai thác lỗi của hãng eEye (Mỹ), nói. "Bạn không nên nghĩ theo chiều hướng rằng phần mềm bảo mật khó khai thác, bởi điều này phụ thuộc vào việc có ai muốn làm điều đó hay không mà thôi".