MCAFEE VÔ TÌNH SỬA MỘT LỖI NGHIÊM TRỌNG

Hãng bảo mật McAfee, cuối tuần qua, cho biết đã khắc phục được một lỗi bảo mật nghiêm trọng trong phần mềm quản lý bảo mật một cách vô tình mà hãng đã không hề nhận ra trước đây. Lỗi bảo mật này ảnh hưởng chủ yếu đến phần mềm ePolicy Orchestrator (ePO) Common Man

Hãng bảo mật McAfee, cuối tuần qua, cho biết đã khắc phục được một lỗi bảo mật nghiêm trọng trong phần mềm quản lý bảo mật một cách vô tình mà hãng đã không hề nhận ra trước đây. Lỗi bảo mật này ảnh hưởng chủ yếu đến phần mềm ePolicy Orchestrator (ePO) Common Management Agent phiên bản 3.5.5 hoặc cũ hơn. Đây là phần mềm quản lý bảo mật được cài đặt trên khoảng 40 triệu PC khác nhau trong các tổ chức lớn. Nếu khai thác thành công lỗi bảo mật này, kẻ tấn công có thể chiếm toàn bộ quyền điều khiển hệ thống bị mắc lỗi. John Viega - phó chủ tịch kiêm kiến trúc sư trưởng bảo mật của McAfee - khẳng định: "Đây là một trong những lỗi bảo mật nghiêm trọng nhất trong sản phẩm của chúng tôi". McAfee đã được eEye Digital Security thông báo cho biết về lỗi bảo mật này từ ngày 5/7. Nhưng trong bản cập nhật phát hành hồi tháng 1 lỗi bảo mật này đã được khắc phục. Tuy nhiên, đó không phải là một bản cập nhật bảo mật mà chỉ là một bản cập nhật nhằm nâng cao hiệu quả hoạt động của phần mềm. "Chúng tôi không hề nhận ra là chúng tôi đã cho khắc phục lỗi bảo mật đó cho đến khi eEye cảnh báo chúng tôi," Viega nói. "Chúng tôi chỉ muốn tối ưu hoá hệ thống phần mềm chứ không có ý định tìm kiếm các lỗi bảo mật. Nhưng thật may chính công việc đó đã giúp chúng tôi khắc phục được một lỗi bảo mật cực kỳ nguy hiểm". McAfee cho biết lỗi bảo mật này không hề ảnh hưởng đến những hệ thống không cài đặt phần mềm quản lý bảo mật. Lỗi bảo mật này phát sinh trong thành phần Framework Service, hãng bảo mật eEye cho biết trong một bản tin cảnh báo phát hành ngày thứ 5 tuần trước. Dịch vụ (service) này mặc được được kích hoạt và vận hành trên tất cả mọi máy chủ và máy khách. "Nếu khai thác thành công, kẻ tấn công có thể ghi một tệp tin có bất kỳ nội dung gì vào bất kỳ đâu trên hệ thống mắc lỗi," eEye khẳng định. Để có thể khai thác được lỗi bảo mật này, kẻ tấn công cần phải truy cập qua mạng vào hệ thống máy khách để gửi đi một thông điệp với định dạng đặc biệt. McAfee khuyến cáo người dùng nên nhanh chóng cài đặt các bản cập nhật phát hành thông qua trang web của hãng. Hoàng Dũng