# BẢN SỬA LỖI CHO APPLE MẮC... LỖI BẢO MẬT

Thật t

Thật trớ trêu khi người ta phát hiện lỗ hổng bảo mật ngay trong chính công cụ dùng để khắc phục các điểm không hoàn thiện trong trình ứng dụng chạy trên nền máy tính Apple.

“Month of Apple Bugs”là dự án gồm các nhà nghiên cứu chủ trương trong suốt tháng giêng năm 2007, mỗi ngày sẽ tìm ra một lỗi bảo mật của phần mềm sử dụng trên các nền máy tính Apple. Hôm thứ hai vừa rồi, các thành viên trong nhóm này công bố họ đã phát hiện một sai sót chết người trong công cụ khắc phục lỗ hổng bảo mật do nhóm sửa lỗi mắc phải.

Phần mềm đó chính là Application Enhancer (gọi tắt là APE), đây là công cụ mà dự án “Month of Apple Fixex” sử dụng để "đắp" các “miếng vá” tức thì ngay khi phát hiện lỗi bảo mật.

APE là loại phần mềm do bên thứ ba phát triển, được thiết kế bởi Unsanity với mục đích “tăng cường và đánh giá lại” cơ chế hoạt động của các trình ứng dụng chạy trên nền máy tính Apple. Cụ thể là APE sẽ tải các plug-in chứa mã thực thi vào những trình ứng dụng đang hoạt động.

Month of Apple Fixes dùng phần mềm này để “vá víu” lại những lỗ hổng mà dự án Month of Apple Bugs phát hiện. Khi ứng dụng chạy, các mảnh vá sẽ tự nhập vào ứng dụng để tìm kiếm các mã sai sót và “trám” vào ngay khi phát hiện lỗ hổng.

Tuy nhiên, hôm thứ hai tuần này Month of Apple Bugs đã công bố một lỗ hổng trong chính APE. Lỗ hổng này cho phép người dùng ở máy cá nhân có thể đoạt được đặc quyền truy cập gốc vào hệ thống, từ đó có thể thay đổi toàn bộ cơ chế hoạt động.

Để làm được điều đó thì hoặc phải sắp xếp lại hệ nhị phân của APE, hoặc là thay thế nó. Theo Month of Apple Bugs, hệ nhị phân của APE được thực hiện bởi các đặc quyền gốc (cấp cao nhất - Root). File này có thể viết như các file khác trong cùng ổ lưu trữ (/Library/Frameworks), do đó sơ hở nói trên sẽ bị lợi dụng để tăng mức đặc quyền truy cập hệ thống.

Ông Landon Fuller, lập trình viên mã nguồn mở kiêm chủ nhiệm dự án Month of Apple Fixes, người luôn sử dụng APE trong công tác của mình, cho rằng, việc xâm chiếm hệ thống từ xa cũng có thể xảy ra. Theo những chia sẻ của ông trên blog cá nhân thì lỗ hổng của APE có thể được kết hợp với việc xâm chiếm từ xa để đoạt đặc quyền truy cập gốc từ một tài khoản administrator mà không cần đến sự tương tác của người dùng. Cũng có một số trường hợp xâm chiếm khác có thể

xảy ra do quyền thay đổi dữ liệu của admin trong các thư mục khác.

Hướng dẫn mọi người cách ứng phó với lỗ hổng này, Month of Apple Bugs cho rằng người dùng không nên sử dụng phần mềm Application Enhancer nữa. Tổ chức này khẳng định, APE "còn sai sót, không chỉ vì cái lỗi trong trường hợp cụ thể này".

Tuy nhiên, ông Fuller phản ứng bằng cách nhấn mạnh lý lẽ cho rằng, đó chỉ là lỗ hổng được chỉ ra về mặt lý thuyết, theo ông việc đoạt quyền truy cập từ xa như thế là không cần thiết. Bất cứ một khai thác APE nào cũng buộc phải kết hợp với một hành vi chiếm dụng từ xa khác thì mới có hiệu quả, còn chỉ cần riêng việc đoạt quyền từ xa thôi cũng đã đủ để dàn xếp cơ chế hoạt động của một máy tính.

Cũng trong blog của mình, ông Fuller thừa nhận: "Lỗ hổng của APE là có thật – do đó một tài khoản administrator trên máy tính cũng có thể đoạt được truyền truy cập gốc bằng cách thay đổi thiết lập của APE mà không cần bất cứ sự khẳng định của người dùng.

Nếu không bị khai thác từ xa, lỗi này cũng có thể được lơi dụng kết hợp với một hành vi khai thác từ xa để giành được các đặc quyền truy cập cao hơn. Tuy nhiên, chỉ riêng việc đoạt quyền từ xa cũng đủ để một hacker truy cập toàn bộ vào cơ sở dữ liệu cá nhân quan trọng của bạn".

Đỗ Dương