HÀNG LOẠT LỖI TRONG SCAN ENGINE BỊ PHÁT HIỆN

Symantec vừa mới cảnh báo người sử dụng về một số lỗ hổng bảo mật nằm trong sản phẩm Scan Engine. Tuy nhiên, hãng bảo mật chỉ xếp những lỗi bảo mật này vào mức trung bình. Scan Engine là một giao diện lập trình cho phép các hãng thứ ba tích hợp công nghệ qu&eac

Symantec vừa mới cảnh báo người sử dụng về một số lỗ hổng bảo mật nằm trong sản phẩm Scan Engine. Tuy nhiên, hãng bảo mật chỉ xếp những lỗi bảo mật này vào mức trung bình. Scan Engine là một giao diện lập trình cho phép các hãng thứ ba tích hợp công nghệ quét diệt phần mềm độc hại của Symantec vào trong các ứng dụng của họ. Theo khuyến cáo của Symantec, lỗi bảo mật thứ nhất nằm trong vấn đề chứng thực đăng nhập web. "Bất kỳ một ai có kiến thức về cơ chế giao tiếp có thể đoạt được quyền kiểm soát máy chủ Scan Engine". Một lỗi bảo mật khác nằm trong việc mở ứng dụng có thể dẫn tới bị tấn công "man-in-the-middle" - một kiểu tấn công ăn cắp thông tin. Theo đó, kẻ tấn công có thể lấy đi các khoá DSA được sử dụng trong giao tiếp an toàn SSL.

Người sử dụng từ xa cũng có thể tải về bất kỳ một tệp tin nào về thư mục cài đặc của chương trình thôgn qua lỗi bảo mật thứ ba. Đây là lỗi sử dụng yêu cầu HTTP độc hại để ăn cắp thông tin. Hãng bảo mật nhấn mạnh rằng những lỗi bảo mật này chỉ ảnh hưởng đến Scan Engine, không ảnh hướng đến bất kỳ ứng dụng nào khác. Người sử dụng được khuyến cáo là nên nâng cấp lên Symantec Scan Engine 5.1 nhằm khắc phục những lỗi bảo mật này. Tính đến nay vẫn chưa có một vụ tấn công nào thông qua việc khai thác các lỗi bảo mật nói trên. Tuy nhiên, đã có những đoạn mã khai thác có khả năng được phát tán trên mạng. HVD - (Betanews)