BẢN TIN NỘI BỘ
CẬP NHẬT VỀ AN TOÀN THÔNG TIN VÀ CẢNH BÁO LỖ HỔNG BẢO MẬT

1. Lỗ hổng trong ứng dụng Outlook cho Android ảnh hưởng đến người dùng

Theo các chuyên gia bảo mật, ứng dụng Outlook với các phiên bản trước 3.0.88 dành cho Android chứa lỗ hổng chèn lệnh và script độc hại (Cross site scripting XSS) mô tả trong CVE-2019-1105 theo các ứng dụng phân tích thông điệp email gửi đến.

Nếu bị khai thác, kẻ tấn công từ xa có thể thực thi mã độc từ phía máy khách trong ứng dụng độc hại trên các thiết bị được nhắm mục tiêu chỉ bằng cách gửi email một tin nhắn được chế tạo đặc biệt.

"Kẻ tấn công khai thác thành công lỗ hổng này sau đó có thể thực hiện các cuộc tấn công XSS trên các hệ thống bị ảnh hưởng và chạy các kịch bản trong bối cảnh bảo mật của người dùng hiện tại."

Theo Microsoft, lỗ hổng được báo cáo là rất nguy hiểm. Các nhà nghiên cứu bảo mật cảnh báo rằng chúng có khả năng dẫn đến các cuộc tấn công giả mạo.

Về các khái niệm, chi tiết về lỗ hổng, các kỹ thuật tấn công hiện vẫn chưa được công khai rộng rãi. Đồng thời Microsoft cũng tuyên bố rằng hiện chưa nắm được thông tin về bất kỳ cuộc tấn công nào trong tự nhiên liên quan đến vấn đề này.

Nếu thiết bị Android của bạn chưa được cập nhật tự động, bạn nên cập nhật thủ công ứng dụng Outlook của mình từ Cửa hàng Google Play để đảm bảo an toàn.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng thiết bị Android cần cập nhật ứng dụng Outlook của mình từ Google Play để đảm bảo an toàn thông tin.

Link tham khảo: https://securitybox.vn/7838/lo-hong-trong-ung-dung-outlook-cho-android-anh-huong-den-hon-100-trieu-nguoi-dung/

2. Phát hiện phương pháp mới cài mã độc đào tiền ảo

Mã độc lén đào tiền ảo lớn nhất được phát hiện là từ hồi tháng 12.2017. Các tin tặc âm thầm xâm nhập vào mạng Wi-Fi cửa hàng Starbucks ở Buenos Aires (Argentina) và phát tán thông qua những người truy cập. Thậm chí, công cụ khai thác này còn được tìm thấy đang chạy quảng cáo trên YouTube thông qua nền tảng DoubleClick của Google và lây lan đến hơn 200.000 thiết bị tại Brazil.

Đến nay, trong một diễn biến mới nhất, các chuyên gia bảo mật từ Trend Micro vừa phát hiện những kẻ tấn công đã khai thác lỗ hổng bảo mật từ máy chủ Oracle WebLogic và cài đặt phần mềm độc hại khai thác đồng tiền ảo Monero (gọi tắt là XMR), đồng thời ẩn thân như một dạng mã hóa gây khó khăn cho các chuyên gia an ninh mạng khi tìm hiểu định dạng.

Trend Micro cũng đã trích dẫn thêm từ các báo cáo từ diễn đàn SANS ISC InfoSec cho biết lỗ hổng này đã bị khai thác từ lâu và cũng đã tiến hành thủ thuật lén đào tiền ảo từ máy tính người dùng.

"Thực chất, dạng tấn công giả mạo các chứng chỉ an toàn không phải là mới, các tin tặc chỉ sử dụng kiểu ngụy trang này cho các cuộc tấn công ẩn danh, bạn hoàn

toàn có thể tránh khỏi được chúng với điều kiện thiết lập an toàn với các chứng chỉ như HTTPs", Trend Micro cho biết.

Theo khuyến cáo của Trend Micro, các công ty đang sử dụng máy chủ Oracle WebLogic phải cập nhật phần mềm bảo mật lên phiên bản mới nhất để tăng thêm mức độ bảo mật cho máy chủ đồng thời ngăn chặn được các nguy cơ thất thoát về tiền điện tử cũng như tài nguyên máy tính của doanh nghiệp.

Ngoài ra, người dùng máy tính cũng cần lưu ý các vấn đề như: Phần trăm CPU usage được sử dụng nhiều hơn bình thường; Quạt làm mát chạy phát ra tiếng ồn như đang chạy chương trình xử lý nặng; Máy tính chậm hẳn mà không rõ nguyên do và RAM bị chiếm dụng nhiều hơn các ứng dụng đang mở.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng không tham gia vào việc đào tiền ảo, luôn đề cao cảnh giác để tránh máy tính bị lợi dụng đào tiền ảo, người quản trị cần cập nhật ngay phần mềm cho máy chủ Oracle WebLogic để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/phat-hien-phuong-phap-moi-cai-ma-doc-dao-tien-ao-1094513.html

3. Kiểm tra email có bị lộ mật khẩu bằng trang web của Cục An toàn thông tin

Sau sự việc 1,4 tỷ tài khoản email bị lộ mật khẩu vừa qua, Cục An toàn thông tin - Bộ TT&TT đã xây dựng trang web https://khonggianmang.vn cho phép người dùng có thể kiểm tra tài khoản thư điện tử của mình có bị lộ hay không.

Theo Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) thuộc Bộ TT&TT, trong 1,4 tỷ tài khoản thư điện tử trên khắp thế giới, Việt Nam có 437.664 tài khoản. Các thông tin tài khoản sử dụng thư điện tử và mật khẩu bị lộ sẽ tạo điều kiện cho tin tặc chiếm đoạt tài khoản và sử dụng vào việc tấn công, đánh cắp và phá hủy hệ thống thông tin, dữ liệu.

Để kiểm tra xem email của mình có bị lộ mật khẩu đợt lộ thông tin của 1,4 tỷ tài khoản email nêu trên không, người dùng có thể truy cập vào trang web https://khonggianmang.vn, nhập địa chỉ mail vào ô "Kiểm tra lộ lọt thông tin tài khoản", sau đó nhấn vào nút "Kiểm tra". Kết quả kiểm tra sẽ được Cục An toàn thông tin gửi tới hộp thư điện tử của người dùng.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng nên kiểm tra việc lộ mật khẩu của email ngoài ra cần tuân thủ các quy định đặt mật khẩu mạnh và đổi mật khẩu theo định kỳ để đảm bảo an toàn thông tin.

Link tham khảo: https://quantrimang.com/kiem-tra-email-co-bi-lo-mat-khau-bang-trang-web-cua-cuc-an-toan-thong-tin-145068

TECHNICAL PAGES:

1. Chi tiết về thông tin một số lỗ hổng trên các sản phẩm/dịch vụ phổ biến tại Việt Nam trong tuần, cụ thể như sau:

STT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2019-0989 CVE-2019-0991 CVE-2019-0993 CVE-2019-1003 CVE-2019-1024 ...	Nhóm 88 lỗ hổng dự trên một số sản phẩm của Microsoft (edge, Office, Windows 10, chakracore ..) cho phép kẻ tấn công truy cập từ xa, chiếm quyền điều khiển, thực thi mã độc.	Đã có thông tin xác nhận và bản vá
2	IBM	CVE-2019-4066 CVE-2019-4067 CVE-2019-4068 CVE-2019-4068 …..	Nhóm 08 lỗ hổng dựa trên một số sản phẩm của IBM (Máy chủ thông tin InfoSphere, IOC, ISIQ) cho phép kẻ tấn công nhúng mã độc JavaScript để lấy thông tin và thay đổi chức năng trong hệ thống, lỗ hổng tiết lộ thông tin nhạy cảm, dữ liệu nhạy cảm không được mã hóa khi truyền đi.	Đã có thông tin xác nhận và bản vá
3	Intel	CVE-2019-0175 CVE-2019-0181 CVE-2019-0164 CVE-2019-0177 ……..	Nhóm 26 lỗ hổng dựa trên một số sản phẩm của Intel (Turbo Boost Max) lỗ hổng bảo vệ mật khẩu ko đủ trong cơ sở dữ liệu cho phép kẻ tấn công lấy thông tin thông qua truy cập cục bộ.	Đã có thông tin xác nhận và bản vá.
4	Linux	CVE-2019-0157 CVE-2019-12818 CVE-2019-10126 CVE-2019-12819 ……	Nhóm 04 lỗ hổng trên một số sản phẩm của Linux (SGX,) cho phép kẻ tấn công từ chối dịch vụ thông qua truy cập cục bộ, tràn bộ đệm.	Đã có thông tin xác nhận và bản vá.
5	Apache	CVE-2018-11800 CVE-2018-11801 CVE-2019-0196 CVE-2019-0197 CVE-2019-0220	Nhóm 05 lỗ hổng trên sản phẩm của Apache (SQL, HTTP Server) cho phép kẻ tấn công thực thi các lệnh SQL tùy ý, xử lý yêu cầu không chính xác.	Đã có thông tin xác nhận và bản vá.

2. Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

STT	Tên miền/IP
1	disorderstatus.ru
2	differentia.ru
3	atomictrivia.ru
4	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
5	klocpdqc7n.ru
6	xjpakmdcfuqe.com
7	646u38k6.ru
8	www.cityofangelsmagazine.com
9	34ksilb9u.ru
10	kodklq.info

3. Các cán bộ kỹ thuật đầu mối về ATTT cần thực hiện:

- Xử lý các lỗ hổng phát hiện tại bảng 1 (nếu có).
- Chặn, xử lý các truy nhập tới các tên miền độc hại tại bảng 2.