BẢN TIN NỘI BỘ

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

1. 50 triệu số điện thoại của người dùng Facebook Việt Nam bị công khai trên mạng

Theo trang TechCrunch, một máy chủ chứa dữ liệu của hơn 419 triệu hồ sơ người dùng Facebook trên toàn thế giới bị rò rỉ trên mạng. Trong số này có 133 triệu người dùng Mỹ, 18 triệu người dùng Anh và hơn 50 triệu người dùng Việt Nam.

Điều đáng nói là máy chủ này không được bảo vệ bằng mật khẩu nào, khiến bất kỳ ai cũng có thể truy cập cơ sở dữ liệu này.

Mỗi hồ sơ chứa một ID người dùng Facebook và số điện thoại được liên kết với tài khoản. Mặc dù số điện thoại người dùng đã không được công khai trong hơn 1 năm trước từ khi Facebook tuyên bố hạn chế quyền này.

TechCrunch đã xác minh một số hồ sơ trong cơ sở dữ liệu bằng cách khớp số điện thoại của người dùng Facebook đã biết với ID Facebook được liệt kê của họ. Ngoài ra, họ cũng kiểm tra các bản ghi khác bằng cách khớp các số điện thoại với tính năng đặt lại mật khẩu Facebook. Một số hồ sơ còn có cả tên người dùng, giới tính và tên quốc gia.

Đây là bê bối bảo mật mới nhất liên quan đến dữ liệu người dùng Facebook sau loạt sự cố kể từ vụ Cambridge Analytica, với hơn 80 triệu hồ sơ người dùng bị lợi dụng trong cuộc bầu cử tổng thống Mỹ năm 2016.

Kể từ đó, Facebook dính hàng loạt sự cố liên quan người dùng, bao gồm cả Instagram, mà hãng này đã thừa nhận.

Vụ rò rỉ số điện thoại mới nhất từ hàng trăm triệu người dùng Facebook này khiến họ đứng trước nguy cơ bị các cuộc gọi spam, quấy rối... Thậm chí tin tặc có thể lừa nhà mạng chuyển số điện thoại của nạn nhân sang điện thoại kẻ tấn công để đặt lại mật khẩu các tài khoản bất kỳ được liên kết với số điện thoại đó.

Sanyam Jain, một nhà nghiên cứu bảo mật và thành viên của GDI Foundation, đã tìm thấy cơ sở dữ liệu trên nhưng không thể tìm ra chủ sở hữu. Khi phóng viên của TechCrunch liên lạc được với máy chủ web, cơ sở dữ liệu này đã bị ngắt kết nối Internet. Jain cho biết, anh đã tìm thấy hồ sơ với số điện thoại của một số người nổi tiếng.

Người phát ngôn của Facebook, Jay Nancarrow cho biết, dữ liệu trên đã bị loại bỏ từ trước khi Facebook tắt quyền truy cập vào số điện thoại của người dùng.

"*Dữ liệu này đã cũ và dường như chúng được thu thập trước khi chúng tôi tắt tính năng tìm kiếm người dùng Facebook qua số điện thoại hồi năm ngoái. Tập dữ liệu này đã bị gỡ và chúng tôi không thấy bằng chứng nào về việc tài khoản Facebook người dùng bị xâm phạm*", Nancarrow cho biết.

Link tham khảo: https://vietnamnet.vn/vn/cong-nghe/bao-mat/hon-50-trieu-so-dien-thoai-cua-nguoi-dung-facebook-viet-nam-bi-cong-khai-tren-mang-565115.html

2. Hàng loạt điện thoại Huawei, LG, Samsung dính lỗ hổng nguy hiểm

Theo Engadget, hãng nghiên cứu bảo mật Check Point đã phát hiện ra lỗ hổng trong điện thoại của Huawei, LG, Samsung và Sony, cho phép kẻ tấn công sử dụng SMS tùy chỉnh để chặn tất cả lưu lượng email trên các thiết bị mục tiêu. Cuộc tấn công sử dụng phiên bản Open Mobile Alliance phổ biến để truy cập email. Các cuộc tấn công yêu cầu những phương thức khác nhau tùy thuộc vào điện thoại và thông tin có sẵn (như số IMSI và yêu cầu mã PIN), nhưng kết quả là như nhau: kẻ xâm nhập lừa người dùng để xâm phạm điện thoại của họ thông qua các tin nhắn thay đổi cài đặt mạng.

Vấn đề bắt nguồn một phần từ cách thức cung cấp hoạt động. Mặc dù nó hỗ trợ cung cấp thông qua các phương thức tương đối an toàn như mã PIN, nhưng nó không yêu cầu chúng. Thường các nhà cung cấp riêng lẻ quyết định cách triển khai định dạng này thay vì những nền tảng như Google, dẫn đến bảo mật không nhất quán. Chẳng hạn, các thiết bị Samsung bị ảnh hưởng không cần bất kỳ xác thực nào để trở thành nạn nhân.

Sự đa dạng này cũng ảnh hưởng đến mức độ an toàn của thiết bị. Một số nhà cung cấp đã giải quyết vấn đề tốt hơn những người khác. Samsung đã sửa lỗi này thông qua bản cập nhật tháng 5, trong khi LG phát hành bản vá vào tháng 7. Tuy nhiên, Huawei cho biết họ sẽ không cung cấp các bản sửa lỗi giao diện, còn Sony "từ chối thừa nhận lỗ hổng" và cho biết họ tuân theo thông số kỹ thuật của Open Mobile Alliance…

Mặc dù các nhà cung cấp nói trên đại diện cho hơn một nửa số điện thoại Android nhưng người dùng có thể tự bảo vệ mình bằng cách từ chối các tin nhắn như mô tả.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng các sản phẩm nêu trên cần cảnh giác với các tin nhắn lạ, luôn cập nhật các bản vá mới nhất của nhà cung cấp để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/hang-loat-dien-thoai-huawei-lg-samsung-dinh-lo-hong-nguy-hiem-1123659.html

3. Firefox 69 vá lỗi thực thi mã nghiêm trọng

Tuần này, Mozilla đã phát hành Firefox 69 vá 20 lỗ hổng, bao gồm một lỗi thực thi mã mức độ nghiêm trọng.

Khi Firefox được khởi động bởi một chương trình khác, các tham số dòng lệnh liên quan đến ghi nhật ký không được xử lý đúng cách. Điều này thường xảy ra khi người dùng nhấp chuột vào một liên kết trong một ứng dụng trò chuyện.

Kẻ tấn công có thể tạo ra các liên kết độc hại, được sử dụng để ghi file vào một vị trí tùy ý, ví dụ thư mục "Startup" của Windows. Lỗ hổng CVE-2019-11751 chỉ ảnh hưởng đến Firefox trên các hệ điều hành Windows.

Theo Trung tâm Bảo mật Internet (CIS): "khai thác thành công […] cho phép thực thi mã tùy ý. Tùy thuộc vào các đặc quyền liên quan đến người dùng, kẻ tấn

công sau đó có thể cài đặt các chương trình; xem, thay đổi, hoặc xóa dữ liệu; hoặc tạo các tài khoản mới với đầy đủ quyền người dùng".

CIS cũng đánh giá rằng, các lỗ hổng này mang lại rủi ro cao cho các tổ chức phi chính phủ/ doanh nghiệp vừa và lớn, nhưng chúng chỉ có tác động trung bình đối với các tổ chức phi chính phủ và doanh nghiệp quy mô nhỏ.

Ngoài ra, Firefox 69 cũng đã xử lý 11 lỗ hổng nghiêm trọng cao, 5 lỗi nguy cơ trung bình và 3 lỗ hổng mức độ nghiêm trọng thấp.

Các vấn đề nghiêm trọng được giải quyết bao gồm CVE-2019-11746 (lỗ hổng use-after-free có thể xảy ra khi thao tác video), CVE-2019-11744 (tấn công XSS do một số thành phần HTML chứa dấu ngoặc mà không được coi là đánh dấu), và CVE-2019-11752 (lỗ hổng use-after-free nằm trong khả năng xóa giá trị khóa IndexedDB và trích xuất trong quá trình chuyển đổi).

Các lỗ hổng khác bao gồm vi phạm chính sách bảo mật same-origin policy (CVE-2019-11742) cho phép đánh cắp hình ảnh cross-origin, thao tác tệp và leo thang đặc quyền với dịch vụ bảo trì Mozilla (CVE-2019-11736), và leo thang đặc quyền với dịch vụ bảo trì Mozilla tại một vị trí cài đặt Firefox tùy chỉnh (CVE-2019-11753).

Mozilla cũng giải quyết một vấn đề qua mặt sandbox trên Firefox Sync (CVE-2019-9812) và cô lập addons.mozilla.org cùng accounts.firefox.com, giúp ngăn chặn thao tác độc hại (CVE-2019-11741).

Các vấn đề nghiêm trọng cao còn lại là lỗi an toàn bộ nhớ, một số lỗi được phát hiện ảnh hưởng đến Firefox ESR 68.1 (CVE-2019-11735), và Firefox ESR 68.1 cũng như Firefox ESR 60.9 (CVE-2019-11740). CVE-2019-11734 chỉ ảnh hưởng tới Firefox 68.

Các lỗ hổng rủi ro trung bình được xử lí trong lần này là CVE-2019-11734 (cross-origin), CVE-2019-11748 (quyền WebRTC trong ngữ cảnh bên thứ ba), CVE-2019-11749 (thông tin camera có sẵn không cần sử dụng getUserMedia), CVE-2019-5849 (ngoài giới hạn đọc trong Skia)…

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng hệ điều hành Windows cần cập nhật phiên bản mới nhất của Firefox để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/firefox-69-va-loi-thuc-thi-ma-nghiem-trong.12682/

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	Adobe	CVE-2019-7968 CVE-2019-7969 CVE-2019-7970 ...	Nhóm 34 lỗ hổng phiên bản sản phẩm của Adobe Photoshop CC cho phép đối tượng tấn công thực thi mã lệnh tùy ý Tuần 34 đã cảnh báo 79 lỗ hổng trong sản phẩm Adobe Acrobat.	Đã có thông tin xác nhận và bản vá.
2	DLink	CVE-2019-15526 CVE-2019-15527 CVE-2019-15528 …..	Nhóm 08 lỗ hổng trên một số sản phẩm của DLink (Router Wifi DIR-823G, DIR-825AC G1) cho phép đối tượng tấn công chèn và thực thi mã lệnh qua nhiều tham số khác nhau, thực hiện, thu thập và chuyển dữ liệu giữa các vùng mạng cô lập khác nhau.	Một số lỗ hổng đã có thông tin xác nhận và bản vá
3	Linux Kernel	CVE-2019-15504 CVE-2019-15505 CVE-2019-15666 ...	Nhóm 05 lỗ hổng nghiêm trọng trong nhân Linux cho phép đối tượng tấn công giả mạo luồng dữ liệu USB, khai thác lỗi Out of Bounds để đọc dữ liệu trên hệ thống, tấn công từ chối dịch vụ Lỗ hổng có điểm CVSS 9.8	Đã có thông tin xác nhận và bản vá
4	Xymon	CVE-2019-13451 CVE-2019-13452 CVE-2019-13455 ...	Nhóm 08 lỗ hổng trên hệ điều hành Xymon cho phép khai thác lỗi tràn bộ đệm để chèn và thực thi mã lệnh. Lỗ hổng có điểm CVSS 7.5	Đã có thông tin xác nhận và bản vá
5	Atlassian	CVE-2019-11589 CVE-2019-8445 CVE-2019-14999 ...	Nhóm 12 lỗ hổng trên một số sản phẩn của Atlassian (Jira,Atlassian Universal Plugin Manager) cho phép đối tượng tấn công khai thác lỗi XSS, CSRF, thu thập thông tin tài khoản người dùng, chuyển	Đã có thông tin xác nhận và bản vá

			hướng người dùng đến trang web độc hại. Một số lỗ hổng đã được cảnh báo trong tuần 34	
6	Ricoh	CVE-2019-14305 CVE-2019-14307 CVE-2019-14308 ...	Nhóm 04 lỗ hổng trên nhiều dòng máy in của Ricoh cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm để chèn và thực thi mã lệnh, từ đó có thể thu thập được nhiều thông tin quan trọng trên các máy in này.	Đã có thông tin xác nhận và bản vá
7	Wordpress	CVE-2015-9372 CVE-2019-15774 CVE-2019-15836 ...	Nhóm 75 lỗ hổng trên nhiều thành phần plugin của Wordpress (Membership Add-on for iThemes Exchange, nd-booking, wp-ultimate-recipe, ...) cho phép đối tượng tấn công khai thác lỗi XSS, CSRF, SQL Injection, sửa đổi thông số cài đặt,	Một số lỗ hổng 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	y3w75xctac.ru
5	xjpakmdcfuqe.com
6	soplifan.ru
7	v99ay4wuo.ru
8	p84epcnjzy.ru
9	xdqzpbcgrvkj.ru
10	ixhtiv.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.