BẢN TIN NỘI BỘ

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

1. Người trẻ tự tin quá mức về bảo mật trên mạng

Trang Marshable ngày 10.5 dẫn khảo sát của Harry Poll thực hiện theo đơn đặt hàng của Google cho thấy người trẻ ngày nay tự tin quá mức về độ an toàn của các tài khoản trên mạng.

Khảo sát được thực hiện đối với 3.000 người ở Mỹ cho thấy khoảng 78% là người thuộc thế hệ Z (16-24 tuổi) thừa nhận rằng họ sử dụng cùng một mật khẩu cho nhiều tài khoản.

"Người dùng trẻ thuộc về thời đại số, họ không nhớ về thời gian chưa có điện thoại thông minh. Tôi nghĩ rằng điều này ảnh hưởng lớn đến nhận thức của họ về công nghệ và an ninh", theo chuyên gia an ninh Emily Schechter của Google.

Thế hệ Baby Boomers (trên 50 tuổi) có khoảng 60% sử dụng cùng 1 mật khẩu cho nhiều tài khoản, trong khi tỷ lệ này là 67% ở nhóm 25-49 tuổi.

Các chuyên gia luôn khuyến cáo không nên sử dụng cùng một mật khẩu cho nhiều tài khoản trên mạng. Bên cạnh đó, mật khẩu dài hơn 8 ký tự, kèm theo số và ký tự đặc biệt sẽ an toàn hơn.

Ngoài ra, người trẻ cũng thiếu cảnh giác trước các thủ đoạn dụ dỗ họ cung cấp thông tin cá nhân (phising) khi 71% tự tin cho rằng họ sẽ không bị lừa, trong khi chỉ 44% hiểu rõ về các thủ đoạn này.

Trong khi đó, 2 nhóm tuổi lớn hơn tỏ ra không tự tin trước các hình thức lừa đảo trên mạng và nhiều người hiểu về phising hơn.

Tuy nhiên, nhiều người thuộc thế hệ Z lại sử dụng biện pháp xác minh 2 bước (76%), so với nhóm Baby Boombers (62%) và thế hệ Y (74%).

"Mọi người không cần là chuyên gia an ninh mạng mới được an toàn. Họ không cần hiểu chứng chỉ an ninh là gì hay nhớ mật khẩu quá phức tạp cho mỗi tài khoản", bà Schechter nói.

Theo chuyên gia này, người dùng cần thiết lập một số điện thoại hoặc email để khôi phục tài khoản và thường xuyên cập nhật, sử dụng mật khẩu khác nhau cho từng tài khoản, thường xuyên cập nhật phần mềm và tiến hành xác minh 2 bước.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng không nên sử dụng một mật khẩu cho các phần mềm và ứng dụng trên mạng, bên cạnh đó cần thiết lập mật khẩu mạnh và thay đổi mật khẩu theo định kỳ để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/gioi-tre/nguoi-tre-tu-tin-qua-muc-ve-bao-mat-tren-mang-1080250.html

2. Bản vá Android tháng 5/2019 khắc phục các lỗ hổng thực thi mã từ xa quan trọng

Các bản vá bảo mật được phát hành vào tháng 5 năm 2019 cho hệ điều hành Android, xử lý 8 lỗ hổng nghiêm trọng, bao gồm 4 lỗ hổng thực thi mã từ xa.

Nghiêm trọng nhất là lỗ hổng trên Media framework, có thể bị khai thác từ xa bằng cách sử dụng tệp đặc biệt để thực thi mã tùy ý trong tiến trình có đặc quyền cao (privileged process).

Lỗ hổng CVE-2019-2044 ảnh hưởng đến hệ điều hành Android 7.0,7.1.1, 7.1.2, 8.0, 8.1 và 9, đã được xử lý trên tất cả các thiết bị cập nhật bản vá Android 2019-05-01.

Các lỗ hổng nghiêm trọng khác được xử lý gồm 3 lỗ hổng thực thi mã từ xa trong System (CVE-2019-2045, CVE-20119-2046, và CVE-2019-2047). Các lỗ hổng này ảnh hưởng đến Android 7.0, 7.1.1, 7.1.2, 8.0, 8.1 và 9.

Năm lỗ hổng khác được vá trong System tháng này bao gồm 2 lỗi leo thang đặc quyền (CVE-2019-2049 và CVE-2019-2050) và 3 lỗi lộ lọt thông tin (CVE-2019-2051, CVE-2019-2052 và CVE-2019-2053). Tất cả năm lỗ hổng này đều được đánh giá ở mức độ nghiêm trọng cao.

Ngoài ra, theo Google, bản vá an ninh trên Android ngày 1/5/2019 đã vá lỗ hổng leo thang đặc quyền có mức độ nghiêm trọng thấp (CVE-2019-2043) trên Framework.

Cũng theo Google, một số vấn đề trên các thành phần Android Kernel, NVIDIA, Broadcom, Qualcomm … cũng được xử lý.

Cụ thể, các lỗi này bao gồm một lỗ hổng leo thang đặc quyền có mức độ nghiêm trọng thấp trên các thành phần Kernel, một lỗ hổng mức độ nghiêm trọng cao trong các thành phần NVIDIA và lỗ hổng thực thi mã từ xa có rủi ro cao trong các thành phần Broadcom.

Hai lỗ hổng trong thành phần Qualcomm được đánh giá có mức độ nghiêm trọng cao.

Bản cập nhật Pixel tháng 5/2019 không có bản vá bảo mật. Tuy nhiên, các thiết bị Pixel sẽ được update sửa lỗi các vấn đề trên Android.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Android cần cập nhật bản vá mới nhất để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/google-va-cac-lo-hong-co-the-khai-thac-tu-xa-tren-android.12238/

3. UC Browser Android - miếng mồi béo bở cho các cuộc tấn công giả mạo URL

Với hơn 600 triệu lượt cài đặt thông qua Play Store, UC Browser và UC Browser Mini Android đang là một trong những nền tảng trình duyệt di động được sử dụng nhiều nhất trên thế giới. Tuy nhiên, trình duyệt này đã không ít lần bị chỉ trích với việc chứa đựng những lỗ hổng nghiêm trọng có thể bị tin tặc khai thác, gây thiệt hại lớn cho người dùng, và phiên bản mới nhất lần này cũng không phải là ngoại lệ. UC Browser và UC Browser Mini Android (phiên bản mới nhất) được cho là có chứa lỗ hổng khiến người dùng dễ dàng trở thành nạn nhân của các cuộc tấn công giả mạo URL. Lỗ hổng này mới đây đã được nhà nghiên cứu bảo mật Arif Khan phát hiện ra và ngay lập tức báo cáo cho đội ngũ bảo mật của UC.

Về cơ bản, các cuộc tấn công giả mạo URL được tiến hành dựa trên khả năng của kẻ tấn công trong việc thay đổi URL hiển thị trên thanh địa chỉ của trình duyệt web nhằm đánh lừa nạn nhân, khiến họ nghĩ rằng trang web mà họ đang truy cập được kiểm soát bởi một bên đáng tin cậy. Như trong trường hợp của lỗ hổng giả mạo URL trên thanh địa chỉ được nhà nghiên cứu Arif Khan phát hiện trong ứng dụng UC Browser cho Android, trang web độc hại thực ra được kiểm soát bởi chính kẻ tấn công.

Nạn nhân có thể bị lừa truy cập vào các miền do kẻ tấn công kiểm soát và ngụy trang dưới dạng những trang web cấu hình cao. Các trang web dạng này sẽ cho phép kẻ tấn công đánh cắp thông tin của nạn nhân bằng cách sử dụng chiến thuật chuyển hướng đến trang đích lừa đảo, hoặc lây nhiễm phần mềm độc hại vào máy tính của họ thông qua các chiến dịch quảng cáo độc hại.

"Có thể nói, giả mạo thanh địa chỉ URL là một trong những hình thức tấn công lừa đảo nguy hiểm nhất hiện nay. Bởi trên thực tế, kiểm tra địa chỉ URL là cách duy nhất để xác định trang web mà người dùng đang truy cập", ông Arif Khan giải thích.

Trong một khuyến cáo bảo mật mới được đăng tải gần đây, nhà nghiên cứu này cũng đã chỉ ra rằng các nền tảng UC Browser và UC Browser Mini có chứa lỗ hổng cho phép kẻ tấn công có thể "đặt tên miền (lừa đảo của mình) làm trang web được nhắm mục tiêu theo cách cực kỳ tinh vi. Ví dụ, một URL hướng tới địa chỉ blogspot.com có thể được hacker biến đổi thành facebook.com chỉ bằng cách điều hướng người dùng truy cập vào địa chỉ www [.] google [.] com [.] blogspot.com [/? q =] www.facebook.com.

"Hình thức tấn công này có thể được thực hiện thành công chủ yếu là bởi vì một số trình duyệt di động như UC Browser và UC Browser Mini hiện đang sử dụng các tính năng kiểm tra regex xấu. Nói cách khác, một số nền tảng trình duyệt di động đang cố gắng nâng cao UX (trải nghiệm người dùng) bằng cách chỉ hiển thị cụm từ tìm kiếm khi người dùng tiến hành tìm kiếm một thông tin gì đó trên các công cụ tìm kiếm như Google chẳng hạn", ông Khan nói thêm.

Cũng theo nhà nghiên cứu này, "Về cơ bản, một số trình duyệt chỉ đơn giản là kiểm tra xem URL mà người dùng đang truy cập có bắt đầu bằng cụm www[.]google[.]com hay không, do đó, kẻ tấn công có thể lợi dụng sự lỏng lẻo này để thể qua mặt tính năng kiểm tra regex và từ đó tước quyền truy cập máy chủ rồi và giả mạo thanh địa chỉ URL".

Trong trường hợp này, để tránh làm lộ người dùng, các nhà phát triển của UC Browser và UC Browser Mini nên loại bỏ các tính năng "cải tiến" của UX, và thiết lập cho trình duyệt phải hiển thị tên miền thực trong mọi trường hợp "nếu họ không thể đưa ra các giải pháp regex tốt hơn hoặc tung ra những tính năng bảo mật hiệu quả đối với chức năng này".

Trong quá trình phân tích, ông Arif Khan nhận thấy một điều khá kì lạ, đó là một số phiên bản UC Browser cũ lại hoàn toàn không dễ bị ảnh hưởng bởi kiểu tấn công trên. Điều này chỉ ra rằng một hoặc thậm chí là một vài trong số những tính

năng mới được thêm vào 2 nền tảng trình duyệt này chính là nguyên nhân gây ra vấn đề.

Bên cạnh đó, ông Arif Khan cũng đã cho đăng tải 2 video bằng chứng (PoC) [UC Browser, UC Browser Mini] cho thấy cách thức những kẻ tấn công có thể lợi dụng lỗ hổng giả mạo thanh địa chỉ để dẫn các nạn nhân tiềm năng đến trang đích lừa đảo hoặc các trang đích có chứa quảng cáo độc hại.

Vấn đề trên được phát hiện trong các phiên bản UC Browser 12.11.2.1184 và UC Browser Mini 12.10.1.1192. Tuy nhiên tại thời điểm viết bài này, công ty phát triển chịu trách nhiệm cho 2 ứng dụng trên là UCWeb vẫn chưa phát hành bản vá hay thậm chí những lời giải thích công khai cho người dùng, mặc dù trên thực tế, vấn đề này đã được ông Arif Khan thông báo tới bộ phận bảo mật của UCWeb một cách chi tiết và cực kỳ có trách nhiệm vào ngày 30 tháng 4 vừa qua. Như vậy, đã gần chục ngày trôi qua mà phía UCWeb vẫn chưa có bất cứ động thái nào để giải quyết vấn đề.

Đặc biệt, sau khi báo cáo của Arif Khan được đăng tải trong các hệ thống của UCWeb, nó đã bị nhóm bảo mật của công ty gán trạng thái "Ignored" (bỏ qua)!

Vào cuối tháng 3 vừa qua, 2 nền tảng trình duyệt Android trên cũng đã bị nhiều nhà nghiên cứu bảo mật chỉ ra rằng chúng có chứa lỗ hổng khiến người dùng dễ dàng trở thành nạn nhân của các cuộc tấn công trung gian (MiTM) bằng cách tải xuống và cài đặt một số mô-đun bổ sung từ máy chủ của chính UCWeb thông qua các kênh không được bảo vệ và đương nhiên là không an toàn, đồng thời bỏ qua các máy chủ của Google Play Store. Sau đó một thời gian ngắn, ngay cả ứng dụng UC Browser cho máy tính để bàn cũng đã bị phát hiện có chứa lỗ hổng tương tự. Tuy nhiên tình huống này được đánh giá là nguy hiểm hơn bởi nó có thể cho phép các tác nhân độc hại âm thầm tải xuống những tiện ích mở rộng chứa mã độc trên máy tính của người dùng.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần gỡ bỏ UC Browser và UC Browser Mini Android cho đến khi có bản cập nhật để đảm bảo an toàn thông tin.

Link tham khảo: https://quantrimang.com/uc-browser-android-bi-tan-cong-gia-mao-url-163577

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	IBM	CVE-2018-2007 CVE-2018-2015 CVE-2018-1961 CVE-2019-4047 CVE-2018-1608 ...	Nhóm 09 lỗ hổng trên một số sản phẩm, ứng dụng của IBM (API Connect, DB2 Linux/ Windows, Rational Engineering Lifecycle Manage, IBM SDK, WebSphere Application Server...) cho phép đối tượng tấn công thực hiện thu thập thông tin, khai thác các lỗi tràn bộ đệm để chèn và thực thi mã lệnh, tấn công leo thang.	Đã có thông tin xác nhận và bản vá
2	Apache	CVE-2019-0213 CVE-2019-0214 CVE-2019-0227 CVE-2019-0194 …..	Nhóm 06 lỗ hổng trong một số sản phẩm của Apache (JMeter, Solr, Qpid Broker-J, Apache Traffic Server) cho phép đối tượng tấn công thực hiện thu thập thông tin, chèn và thực thi mã lệnh trong phạm vi của ứng dụng.	Đã có thông tin xác nhận và bản vá
3	Mozilla	CVE-2019-9791 CVE-2019-9792 CVE-2019-9794 CVE-2019-9795 ……..	Nhóm 31 lỗ hổng dựa trên một số sản phẩm của Mozilla (Thunderbird…) cho phép kẻ tấn công có quyền truy cập và thực thi vào hệ thống qua nhiều giao thức khác nhau gây ra thiếu dữ liệu.	Đã có thông tin xác nhận và bản vá.
4	Dell	CVE-2019-3705 CVE-2019-3706 CVE-2019-3707 ……	Nhóm 03 lỗ hổng trên một số sản phẩm của Dell (ECM iDRAC) cho phép đối tượng tấn công thực thi và khai thác các lỗi tràn bộ nhớ đệm để chèn và thực thi mã lệnh độc. Ảnh hưởng đến các phiên bản iDRAC6/7/8/9.	Đã có thông tin xác nhận và bản vá.

5	Zohocorp	CVE-2013-7470 CVE-2011-3151 CVE-2019-11486 CVE-2019-11487 …….	Nhóm 04 lỗ hổng trên sản phẩm của Zohocorp cho phép đối tượng tấn công thực thi đặt các tập tin trojan vào hệ thống, tấn công XSS, SQL Injection	Chưa có thông tin xác nhận và chưa có bản vá

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

STT	**Tên miền/IP**
1	43trfdsds.com
2	strikotunrev.top
3	d3s1.me
4	io90s8dudi.xyz
5	tesivisi11.top
6	laopre.at
7	babushkabenmen.net
8	strikotunrev.top
9	pupuiolili.top
10	dnshkjashsdk3d11144d.ru

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.