BẢN TIN NỘI BỘ

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

1. UC Browser mắc lỗi bảo mật ảnh hưởng hàng triệu người dùng Android

Nếu thường xuyên sử dụng trình duyệt UC Browser của Alibaba, bạn nên dừng việc đó vào lúc này.

Theo SlashGear, một nhóm nghiên cứu bảo mật và công ty Dr. Web Anti-Virus đã phát hiện UC Browser có khả năng "đi đường vòng" qua máy chủ của Google Play để tải thêm các mô-đun phần mềm và thư viện tập tin, từ đó tạo cơ hội cho mã độc xâm nhập. Đáng lo ngại nhất là cách mà trình duyệt này bảo mật máy chủ điều khiển, được mô tả là chẳng khác gì "lạy ông tôi ở bụi này".

Việc đi vòng qua máy chủ và quy trình xác thực của Google rõ ràng đã vi phạm nguyên tắc của Google Play, vốn ngăn cản các ứng dụng tải thêm tập tin từ những nguồn khác ngoài chợ ứng dụng này. Dr. Web chỉ ra rằng UC Browser đã áp dụng cách thức rủi ro được đề cập từ năm 2016.

UC Browser còn sử dụng giao thức truyền tải không được mã hóa là HTTP, thay vì HTTPS (an toàn hơn), tạo điều kiện cho kẻ xấu thực hiện kiểu tấn công man-in-the-middle. Tin tặc có thể can thiệp vào quá trình truyền tải dữ liệu để tuồn mã độc vào ứng dụng, đẩy người dùng vào kịch bản bị lừa đảo hoặc tệ hơn nữa.

Trình duyệt này sẽ khởi chạy bất cứ thứ gì nó tải xuống, vì không hề có bất kỳ phương thức xác thực tập tin hay plugin nào được áp dụng.

UC Browser đạt hơn 500 triệu lượt tải nên lỗ hổng bảo mật này chắc chắn khiến hàng triệu người dùng gặp rủi ro. Dr. Web cũng lưu ý phiên bản thu gọn của trình duyệt là UC Browser Mini, với hơn 100 triệu lượt tải, cũng có vấn đề tương tự.

Dr. Web đã báo cáo thông tin cho nhà phát triển ứng dụng và Google, nhưng ngay tại thời điểm họ công bố báo cáo thì cả hai ứng dụng trên vẫn còn hiện diện trên Google Play Store. Trong khi chờ đợi phản hồi, Dr. Web khuyên người dùng gỡ bỏ cài đặt UC Browser để phòng tránh rủi ro bị tấn công

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng Android cần gỡ bỏ trình duyệt UC Browser để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/uc-browser-mac-loi-bao-mat-anh-huong-hang-trieu-nguoi-dung-android-1065144.html

2. Cảnh báo: Máy chủ cập nhật phần mềm ASUS bị hack để phát tán mã độc

Một nhóm hacker được nhà nước bảo trợ đã tìm cách chiếm quyền điều khiển máy chủ cập nhật phần mềm tự động ASUS Live trong khoảng thời gian từ tháng 6 đến tháng 11 năm 2018 và đẩy bản cập nhật độc hại để cài backdoor trên hơn 1 triệu máy tính Windows trên toàn thế giới.

Theo các nhà nghiên cứu bảo mật từ công ty Kaspersky Lab, người đã phát hiện ra cuộc tấn công và đặt tên là Shadow Hammer. ASUS đã được thông báo về cuộc tấn công ngày 31 tháng 1 năm 2019.

Sau khi phân tích hơn 200 mẫu cập nhật độc hại, các nhà nghiên cứu tin rằng hacker không muốn tấn công vào tất cả người sử dụng, thay vào đó chỉ có một danh sách người dùng được xác định bởi địa chỉ MAC được hardcode vào phần mềm độc hại.

Tương tự các vụ CCleaner và ShadowPad bị hack, file độc hại được ký bởi chữ ký số hợp pháp của ASUS để làm cho nó giống một bản cập nhật phần mềm từ công ty và không bị phát hiện trong thời gian dài.

Các nhà nghiên cứu không quy kết cho bất kỳ nhóm tấn công APT nào tại thời điểm này, nhưng một số bằng chứng nhất định cho thấy có liên quan đến vụ tấn công ShadowPad năm 2017, mà Microsoft quy cho BARIUM APT.

Khuyến nghị:

Phòng ATTT khuyến nghị: Hiện bản cập nhật mới nhất của Asus đã xử lý được vấn đề này. Người dùng Asus cần cập nhật các phần mềm Asus mới nhất để bảo đảm an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/canh-bao-may-chu-cap-nhat-phan-mem-asus-bi-hack-de-phat-tan-ma-doc.12098/

3. Dữ liệu khách hàng của Toyota Việt Nam bị tấn công

Công ty ô tô Toyota Việt Nam vừa chia sẻ thông tin phát hiện ra việc có khả năng bị tấn công mạng và một số dữ liệu khách hàng có thể đã bị truy cập.

Không chỉ có Toyota Việt Nam mà cả Toyota Nhật Bản, Toyota Mỹ, Toyota Thái Lan, Toyota Úc đồng loạt bị tấn công mạng. Tập đoàn này phát hiện ra việc mạng bị tấn công nhưng chưa rõ nguyên nhân vụ việc và những thiệt hại.

"Đến nay chúng tôi chưa có bất cứ bằng chứng cụ thể và chi tiết về các dữ liệu bị mất, hiện đang trong quá trình điều tra", đại diện Toyota Việt Nam thông báo và lấy làm tiếc cho các ảnh hưởng có thể xảy ra với các đối tác liên quan.

Với Toyota Việt Nam, công ty này đã báo cáo các cơ quan chức năng để hỗ trợ điều tra vụ tấn công.

Theo các chuyên gia công nghệ thông tin, Toyota là tập đoàn ô tô có số lượng khách hàng lớn và dữ liệu khách hàng, có thể là đích ngắm của những kẻ tấn công mạng.

Ông Tuấn Anh, Phó Tổng giám đốc BKAV, cho biết, các tin tặc đang chủ động tấn công vào hệ thống dữ liệu lớn. Các hệ thống dữ liệu đều kết nối Internet và những lỗ hổng an ninh thường xuyên xuất hiện và tin tặc luôn luôn theo dõi. Một hệ thống mạng bao giờ cũng có tường lửa để bảo vệ, nhưng chính nó cũng tồn tại những lỗ hổng và kẻ tấn công khi phát hiện ra sẽ nhanh chóng khai thác.

Tuy là tấn công mạng, trên môi trường ảo, nhưng thiệt hại là thật. Ví dụ, một doanh nghiệp khi bị tin tặc tấn công đánh cắp hoặc xóa sạch hệ thống dữ liệu khách hàng thì thiệt hại vô cùng lớn. Chắc chắn doanh số sẽ giảm mạnh, uy tín bị ảnh hưởng nặng nề.

Vụ việc hơn 5,4 triệu thông tin cá nhân, được cho là khách hàng của Thế giới Di động, bị đăng tải công khai trên mạng vào tháng 10/2018 là ví dụ. Tuy thiếu căn

cứ khẳng định bị tin tặc tấn công, đánh cắp, nhưng thiệt hại về kinh tế của DN này là có thật. Thế giới Di động cũng rất mệt mỏi khi giải quyết vụ khủng hoảng. Trên thị trường chứng khoán, ngay lập tức cổ phiếu MWG của Thế giới Di động bị ảnh hưởng và giá tụt giảm.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng và quản trị cần tuân thủ chính sách an toàn thông tin của đơn vị, cập nhật các bản vá đối với thiết bị để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/du-lieu-khach-hang-cua-toyota-viet-nam-bi-tan-cong.12113/

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-2017-1713 CVE-2019-4052 CVE-2019-4094 CVE-2018-1992 CVE-2018-1836 ...	Nhóm 05 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-2018-11767 CVE-2018-11789 CVE-2019-0191 ...	Nhóm 03 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	Rdesktop	CVE-2018-20177 CVE-2018-20179 CVE-2018-20181 CVE-2018-20182 CVE-2018-20174 CVE-2018-20175 CVE-2018-20176 CVE-2018-20178 ...	Nhóm 08 lỗ hổng trong phần mềm Rdesktop (phần mềm Remote Desktop thường sử dụng trên các hệ điều hành Linux) cho phép khai thác nhiều lỗi khác nhau trong đó có nhiều lỗi tràn bộ đệm để chèn và thực thi mã lệnh. Ảnh hưởng tới các phiên bản Rdesktop 1.8.3 và các phiên bản trước đó; FreeRDP phiên bản 2.0.0-rc4 và các phiên bản trước đó.	Đã có thông tin xác nhận và bản vá.
4	Putty	CVE-2019-9895 CVE-2019-9898 CVE-2019-9894 CVE-2019-9896 CVE-2019-9897 …	Nhóm 05 lỗ hổng trong Putty những kẻ tấn công lợi dụng các phiên bản PuTTY trước 0,71 chiếm quyền điều khiển các ứng dụng bằng cách đặt 1 tệp tin trợ giúp độc hại trong cùng thư mục với tệp thực thi. Trong các phiên bản PuTTY trước 0,71 trên Unix, tràn bộ đệm có	Chưa có thông tin xác nhận và bản vá.

			thể kích hoạt từ xa tồn tại trong bất kỳ loại chuyển tiếp từ máy chủ đến máy khách nào	
5	Cisco	CVE-2019-1716 CVE-2019-1766 CVE-2019-1765 CVE-2019-1764 CVE-2019-1763 …	Nhóm 05 lỗ hổng trên một số sản phẩm của Cisco (các dòng switch Nexus, NX-OS, FXOS Software,) cho phép truy cập và thông tin nhạy cảm lưu trữ trên hệ thống, chèn và thực thi mã lệnh để chiếm quyền kiểm soát thiết bị.	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	plpanaifheaighai.com
2	n.hmiblgoja.ru
3	ajkeahkcueafuiaeuf.ru
4	mokoaehaeihgiaheih.ru
5	iuefgauiaiduihgs.com
6	mel.cloudcontentsmak.com
7	43trfdsds.com
8	bszotsjovih.com
9	9 strikotunrev.top
10	kisscherrygirls.com

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.