BẢN TIN NỘI BỘ

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

1. Google vá lỗ hổng nghiêm trọng trong Android

Google vừa phát hành bộ bản vá an ninh mạng đầu tiên cho Android trong năm 2019, xử lý hơn 20 lỗ hổng.

Lỗ hổng nghiêm trọng nhất là CVE-2018-9583, một lỗ hổng thực thi mã từ xa nghiêm trọng được xử lý trong hệ thống và bao gồm trong gói bản vá 2019-01-01.

Gói bản vá 2019-01-01 xử lý tổng cộng 13 vấn đề an ninh ảnh hưởng đến nền tảng và hệ thống.

Lỗ hổng duy nhất được xử lý trong nền tảng là lỗi leo thang đặc quyền CVE-2018-9582. Lỗ hổng được đánh giá ở mức nghiêm trọng cao và ảnh hưởng đến các phiên bản Android 8.0, 8.1 và 9.

Tất cả 12 lỗ hổng còn lại đều ảnh hưởng đến hệ thống: 1 lỗi thực thi mã từ xa quan trọng, 4 lỗi leo thang đặc quyền ở mức nghiêm trọng cao và 7 lỗ hổng tiết lộ thông tin cũng ở mức nghiêm trọng cao. Các phiên bản Android bị ảnh hưởng bao gồm 7.0, 7.1.1, 7.1.2, 8.0, 8.1 và 9.

Gói bản vá thứ 2 là 2019-01-05, xử lý 14 lỗ hổng trong các thành phần Kernel, các thành phần NVIDIA, các thành phần Qualcomm và các thành phần nguồn đóng Qualcomm.

Hầu hết các lỗi này đều ở mức nghiêm trọng cao, ngoại trừ CVE-2018-11847, một lỗi cực kỳ nghiêm trọng được xử lý trong thành phần nguồn đóng Qualcomm. Còn lại hầu hết là lỗ hổng leo thang đặc quyền.

Theo Google, lỗ hổng nghiêm trọng nhất trong số các lỗ hổng này có thể cho phép các ứng dụng nội bộ độc hại thực thi mã tùy ý trong bối cảnh của một quy trình đặc quyền.

Cũng trong tuần này, Google đã phát hành bản cập nhật an ninh cho các thiết bị Pixel/Nexus, xử ly 2 lỗ hổng ở mức nghiêm trọng trung bình trong các thành phần Kernel, CVE-2018-13098 và CVE-2018-13099. Đây đều là 2 lỗi lộ lọt thông tin.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng các thiết bị Android cần cập nhật phiên bản mới nhất để tránh nguy cơ mất an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/google-va-lo-hong-nghiem-trong-trong-android.11906/

2. Nhiều ứng dụng trên App Store đang kết nối với máy chủ độc hại

Hãng bảo mật Wandera đã phát hiện ra 14 trò chơi đều giao tiếp với cùng một máy chủ có liên kết đến phần mềm độc hại Golduck từng xuất hiện trên Android.

Theo Engadget, Wandera ghi nhận các ứng dụng này được thiết kế để tải quảng cáo, nhiều khả năng nhằm đánh lừa người dùng cấp quyền cho phần mềm độc hại được cài đặt bên ngoài App Store. Ghi nhận từ Wandera cho thấy 14 ứng dụng này

đã được tải xuống gần 1 triệu lần, có nghĩa rất nhiều người đang đối diện với phần mềm độc hại.

Hiện tại, Apple vẫn chưa có bình luận nào về vấn đề, nhưng quyền truy cập vào các ứng dụng hiện bị hạn chế. Nó vẫn có trên App Store nhưng được liệt kê không có sẵn ở Mỹ như là cách để ngăn ngừa mã độc lan rộng ra bên ngoài.

Được biết Golduck là một dạng malware cắm mã cổng hậu vào phần mềm để đánh cắp thông tin và kiểm soát thiết bị. Hơn 10 triệu người dùng Android từng nhiễm malware này, tạo điều kiện cho tin tặc chiếm quyền điều khiển thiết bị, gửi tin nhắn SMS từ điện thoại nạn nhân ra bên ngoài để kiếm tiền.

Các nhà nghiên cứu khuyến cáo người dùng cần cảnh giác với loại phần mềm độc hại, ngay cả với thiết bị iOS. Để an toàn, hãy chỉ tải ứng dụng đến từ App Store được thiết kế chống lại phần mềm độc hại rất tốt.

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng thiết bị IOS cần cảnh giác với các phần mềm lạ, chỉ cài các ứng dụng đã được đảm bảo trên App Store để đảm bảo an toàn thông tin.

Link tham khảo: https://thanhnien.vn/cong-nghe/nhieu-ung-dung-tren-app-store-dang-ket-noi-voi-may-chu-doc-hai-1041624.html

3. Patch Tuesday tháng 01/2019 của Microsoft tập trung vào lỗi thực thi mã từ xa

Bản cập nhật Patch Tuesday đầu tiên năm 2019 của Microsoft chủ yếu khắc phục các lỗ hổng thực thi mã từ xa (RCE), với gần một nửa trong tổng số 47 bản vá lỗi tập trung vào RCE. Các doanh nghiệp cũng được khuyến cáo cập nhật bản vá hồi tháng 12/2018 cho Internet Explorer sau các cuộc tấn công trong thực tế.

Bảy lỗ hổng được xếp hạng Nghiêm trọng, 40 lỗ hổng Quan trọng và hai lỗi mức Trung bình. Các bản vá lỗi được phát hành cho Internet Explorer, Microsoft Edge, Windows, Office, Office Services và Web Apps, ChakraCore, Visual Studio và .NET Framework.

Như chuyên gia Dustin Childs của Trend Micro chỉ ra trong một bài đăng trên blog, số lỗ hổng RCE chiếm một nửa số lỗi được xử lý cho tháng 1 năm 2019. Mười một lỗ hổng trong số này liên quan đến hệ quản trị cơ sở dữ liệu Jet Database Engine. Một lỗ hổng (CVE-2019-0579) đã được biết đến công khai và được xếp hạng quan trọng. Microsoft cho biết khai thác lỗ hổng này có thể cho phép kẻ tấn công thực thi mã tùy ý trên hệ thống nạn nhân. Điều này đòi hỏi tương tác của người dùng; đối tượng mục tiêu sẽ phải mở một file được tạo đặc biệt để thực thi.

Mặc dù chỉ được đánh giá quan trọng, nhưng việc tiết lộ lỗ hổng này có nghĩa là kẻ tấn công có thể phát triển bộ khai thác lỗ hổng dễ dàng hơn.

Cũng được ưu tiên cao là CVE-2019-0547, một lỗ hổng RCE trong máy khách Windows DHCP. Một lỗi bộ nhớ tồn tại trong máy khách khi kẻ tấn công gửi phản hồi DHCP được tạo đặc biệt cho máy khách. Khai thác thành công sẽ cho phép kẻ tấn công thực thi mã tùy ý trên máy khách.

Childs cho biết: "Microsoft đánh giá chỉ số khai thác Exploit Index cao nhất, có nghĩa là lỗi này có khả năng khai thác cao". Ông lưu ý rằng lỗ hổng này nằm trong phiên bản Windows mới nhất nhưng không có trong các phiên bản trước đó, có thể là do thành phần được viết lại cho các hệ thống mới hơn.

"Nếu bạn đang chạy Windows 10 hoặc Server phiên bản 1803, bản vá này phải đứng đầu danh sách triển khai của bạn", Childs viết.

Một lỗi Office khác (CVE-2019-0560), được tìm thấy bởi Mimecast, có thể cho phép rò rỉ dữ liệu ngoài ý muốn trong các tài liệu và tệp Office được tạo trước đó. Mặc dù khó sử dụng nó như một lỗ hổng thực thi mã, nhưng nó có thể được sử dụng để thu thập dữ liệu mà người dùng vô tình để lộ.

"Mặc dù chắc chắn có thể khai thác lỗ hổng này để thực hiện một cuộc tấn công thực thi từ xa, nhưng điều này sẽ đòi hỏi chuyên môn kỹ thuật tương đối cao từ phía kẻ tấn công", Matthew Gardiner, chiến lược gia an ninh tại Mimecast cho biết.

Đáng chú ý trong tháng này là CVE-2018-8653, một bản vá lỗi out-of-band (lỗi ngoài dải băng tần) được Microsoft ban hành cho một lỗi bộ nhớ trong Internet Explorer vào tháng 12 năm 2018. Microsoft cho biết, khai thác lỗ hổng này kẻ tấn công có thể thực thi mã tùy ý trong ngữ cảnh người dùng hiện tại và có được quyền tương tự như của người dùng.

"Lỗ hổng tiếp tục được khai thác trong thực tế và công ty công nghệ Recorded Future đã chứng kiến một số bộ công cụ khai thác cùng các proof of concept được phát hành trên nền tảng của họ", Allan Liska, kiến trúc sư giải pháp cao cấp của Recorded Future cho biết. "Nếu bạn chưa vá lỗ hổng này, nó sẽ là ưu tiên số 1".

Khuyến nghị:

Phòng ATTT khuyến nghị: Người dùng cần cập nhật phiên bản mới nhất do Microsoft khuyến cáo để đảm bảo an toàn thông tin.

Link tham khảo: https://whitehat.vn/threads/patch-tuesday-thang-1-2019-cua-microsoft-tap-trung-vao-loi-thuc-thi-ma-tu-xa.11902/

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	Apache Netbeans	CVE-2018-17191 …	Lỗ hổng trong Apache Netbeans (Môi trường phát triển các ứng dụng Java) cho phép đối tượng tấn công chèn và thực thi mã lệnh. Có thể cập nhật lên Netbean10.0	Đã có thông tin xác nhận và bản vá
2	F5	CVE-2018-15334 CVE-2018-15335 CVE-2018-17539 ...	Nhóm 04 lỗ hổng trên một số sản phẩm của F5 (BIG-IP APM) cho phép đối tượng tấn công thực hiện cho phép đối tượng tấn công khai thác lỗi CSRF, tấn công từ chối dịch vụ, người dùng Guest có thể truy cập và xóa tập tin tùy ý bao gồm cả những tập tin cấu hình.	Đã có thông tin xác nhận và bản vá
3	Fasterxml Jackson	CVE-2018-14718 CVE-2018-19360 CVE-2018-14720 ...	Nhóm 07 lỗ hổng trên bộ thư viện Fasterxml Jackson cho phép đối tượng tấn công thực hiện mã lệnh tùy ý thông qua một số thành phần (slf4j-ext, blaze-ds-opt, -corejars), khai thác lỗi SSRF (trong thành phần axis2-jaxws).	Đã có thông tin xác nhận
4	Foxit	CVE-2019-5007 CVE-2019-5006 CVE-2019-5005	Nhóm 03 lỗ hổng trên Foxit Foxit Reader và PhantomPDF (phiên bản cho hệ điều hành Windows) cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm	Đã có thông tin xác nhận và bản vá
5	FreeBSD	CVE-2018-17161	Lỗ hổng trong một số phiên bản của hệ điều hành FreeBSD cho phép đối tượng tấn công khai thác lỗi tràn bộ đệm để chèn và thực thi mã lệnh.	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	q4dgp6xv.ru
5	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
6	xjpakmdcfuqe.com
7	9lnbo2e3.ru
8	www.cityofangelsmagazine.com
9	dqrzxapnw.info
10	caarmelcollege.org

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.